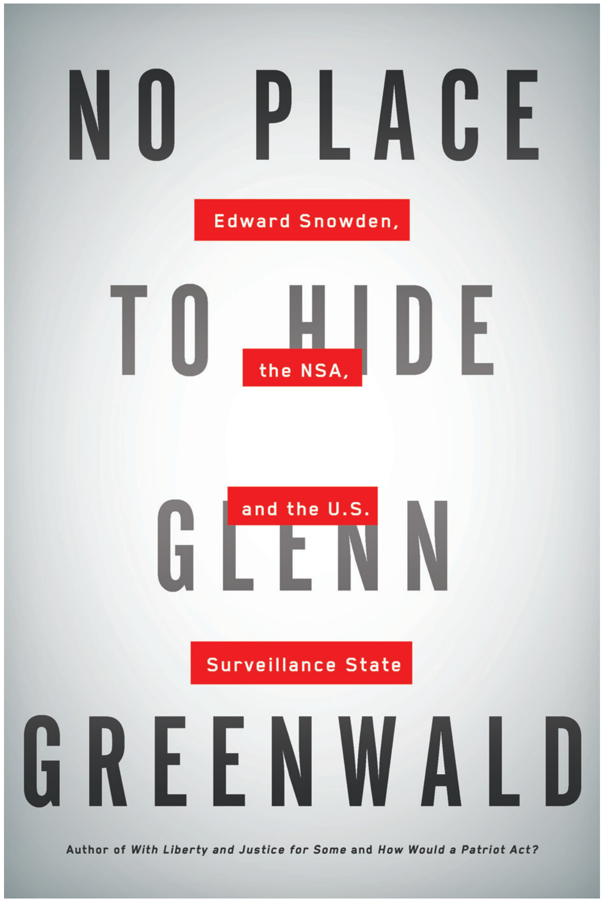
DOCUMENTS FROM *NO PLACE TO HIDE*

Glenn Greenwald's *No Place to Hide* includes the following documents from the Snowden archive. For discussion of these documents, please see the book at the page numbers indicated.



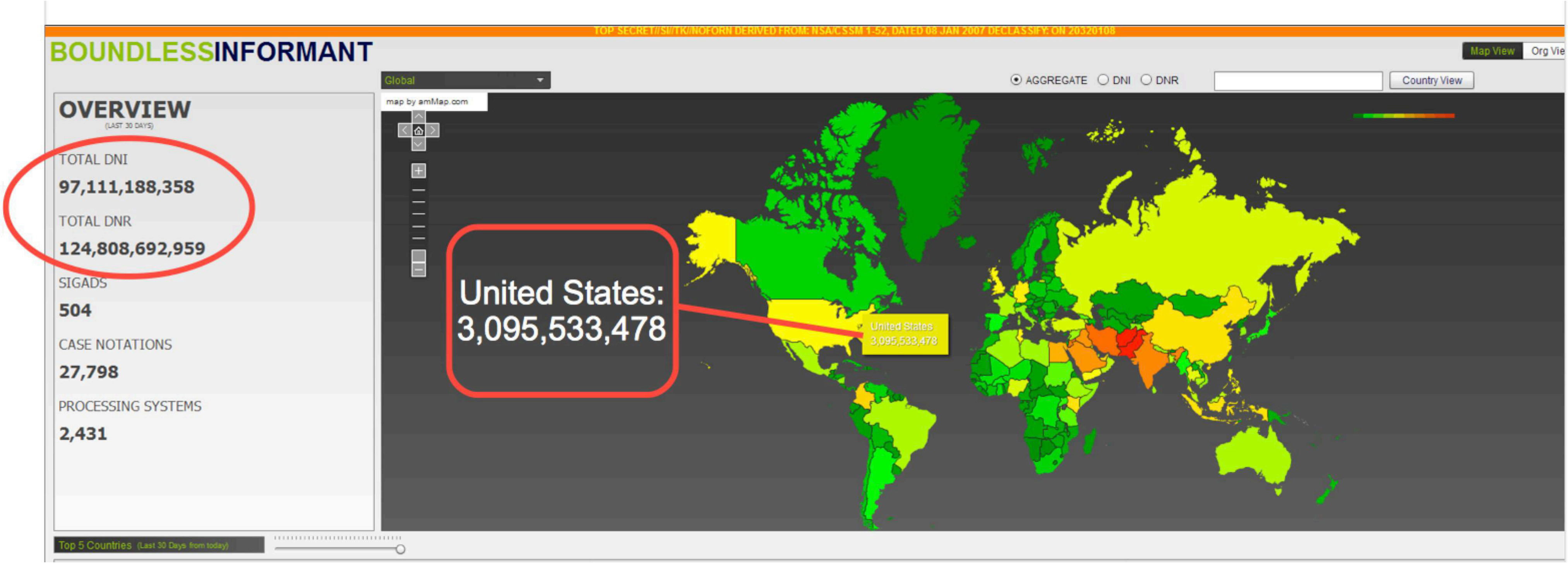
BUY THE BOOK:

amazon.com BARNES&NOBLE INDIEBOUND macmillan

E-BOOK

amazonkindle iBooks kobo nook

GLENNGREENWALD.NET



TOP SECRET//SI//TK//NOFORN DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY: ON 20320108

BOUNDLESSINFORMANT

OVERVIEW
(LAST 30 DAYS)

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

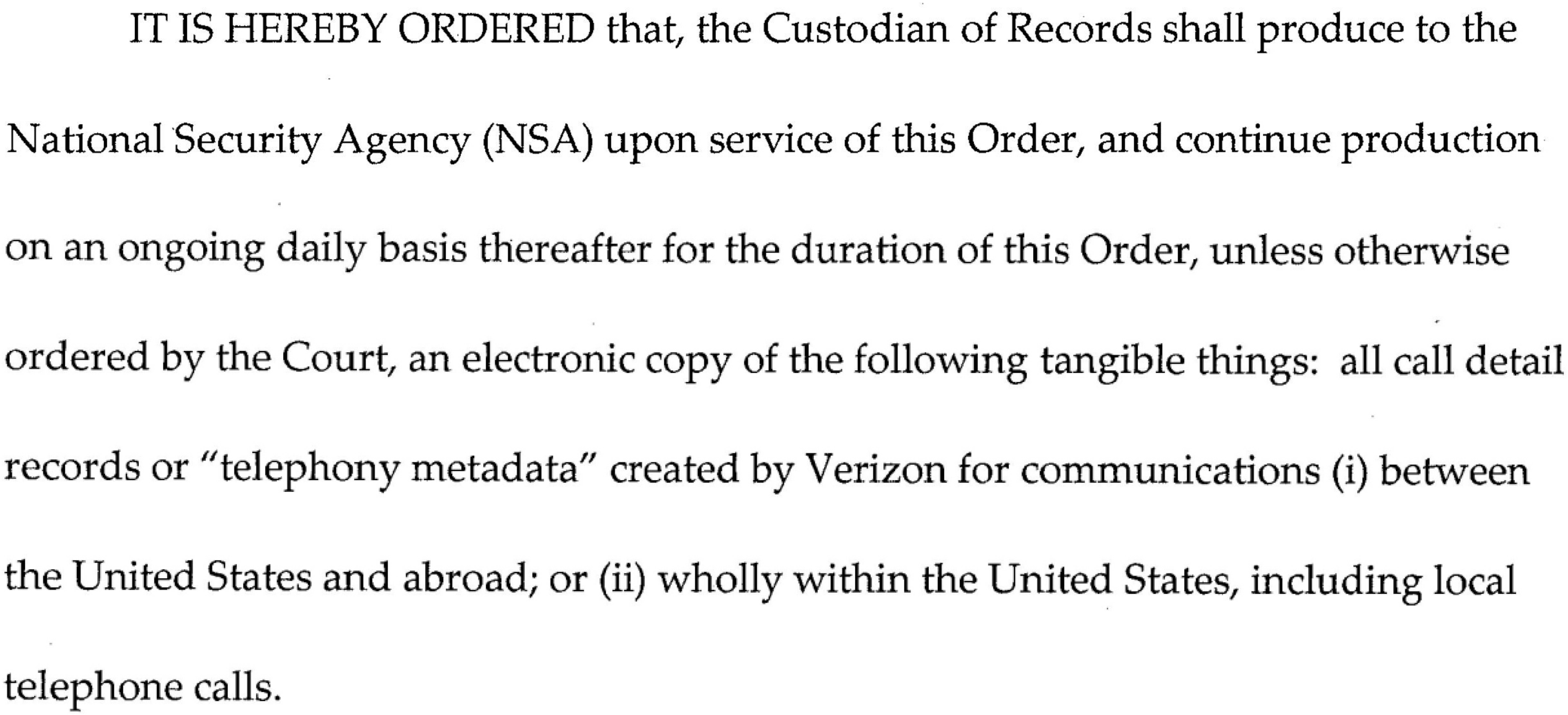
SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431

United States:
3,095,533,478

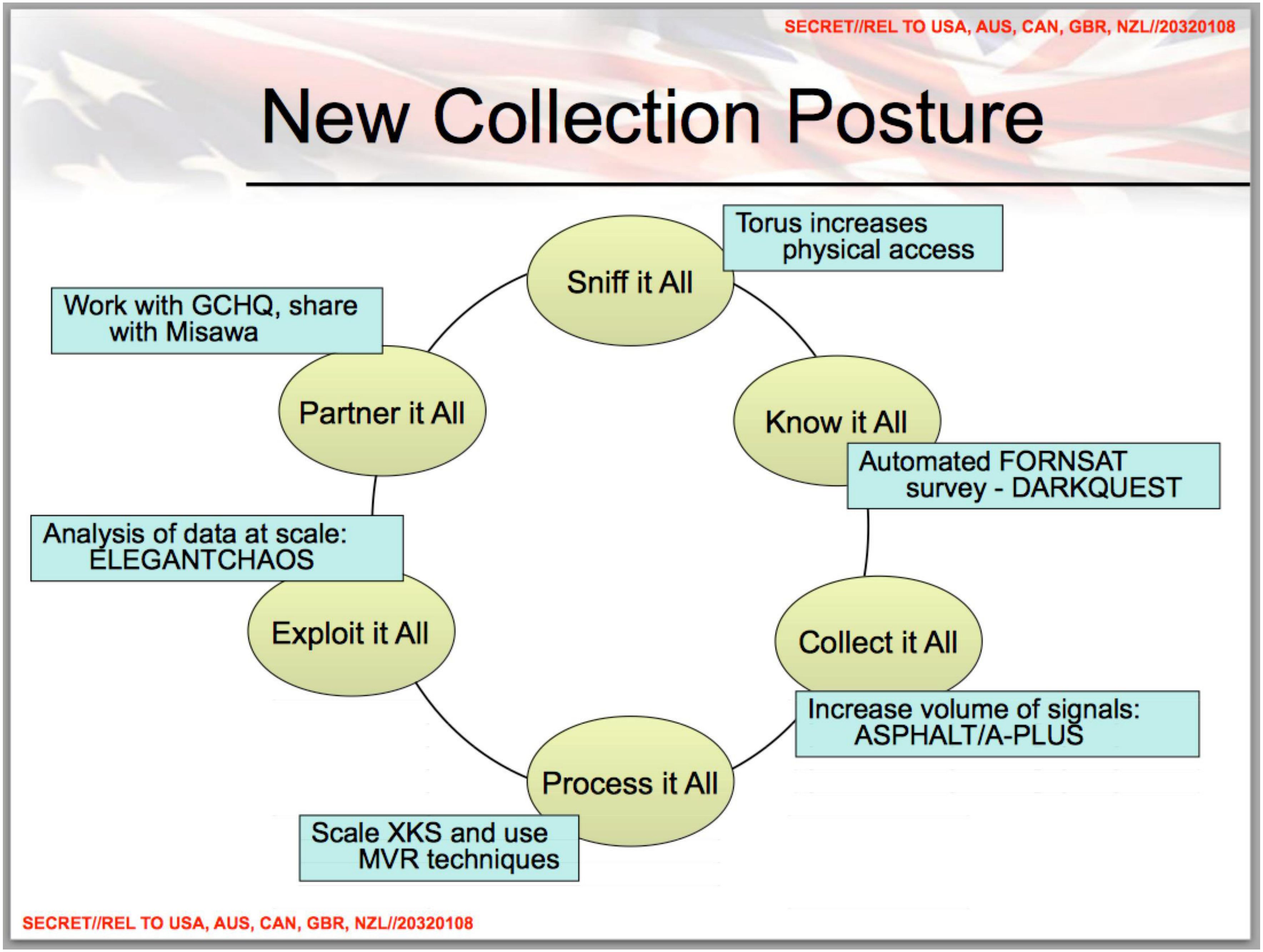
Top 5 Countries (Last 30 Days from today)



IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

(Continued)

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

New Collection Posture

Sniff it All

Torus increases physical access

Know it All

Automated FORNSAT survey - DARKQUEST

Collect it All

Increase volume of signals: ASPHALT/A-PLUS

Process it All

Scale XKS and use MVR techniques

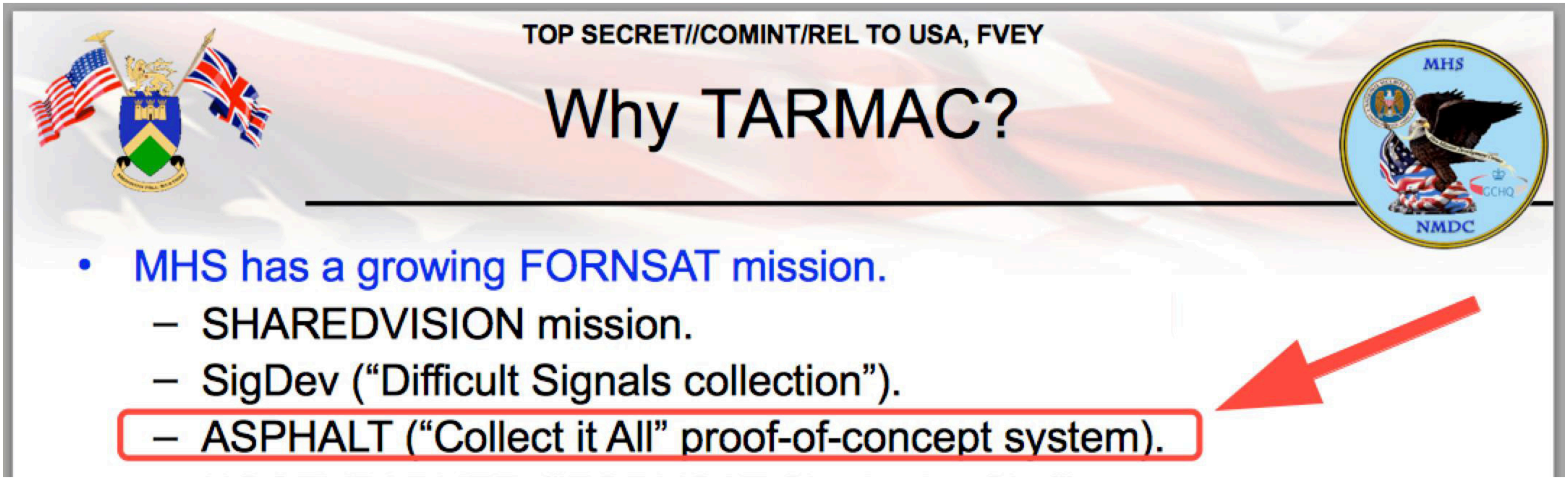
Exploit it All

Analysis of data at scale: ELEGANTCHAOS

Partner it All

Work with GCHQ, share with Misawa

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



TOP SECRET//COMINT/REL TO USA, FVEY

MHS
GCHQ
NMDC

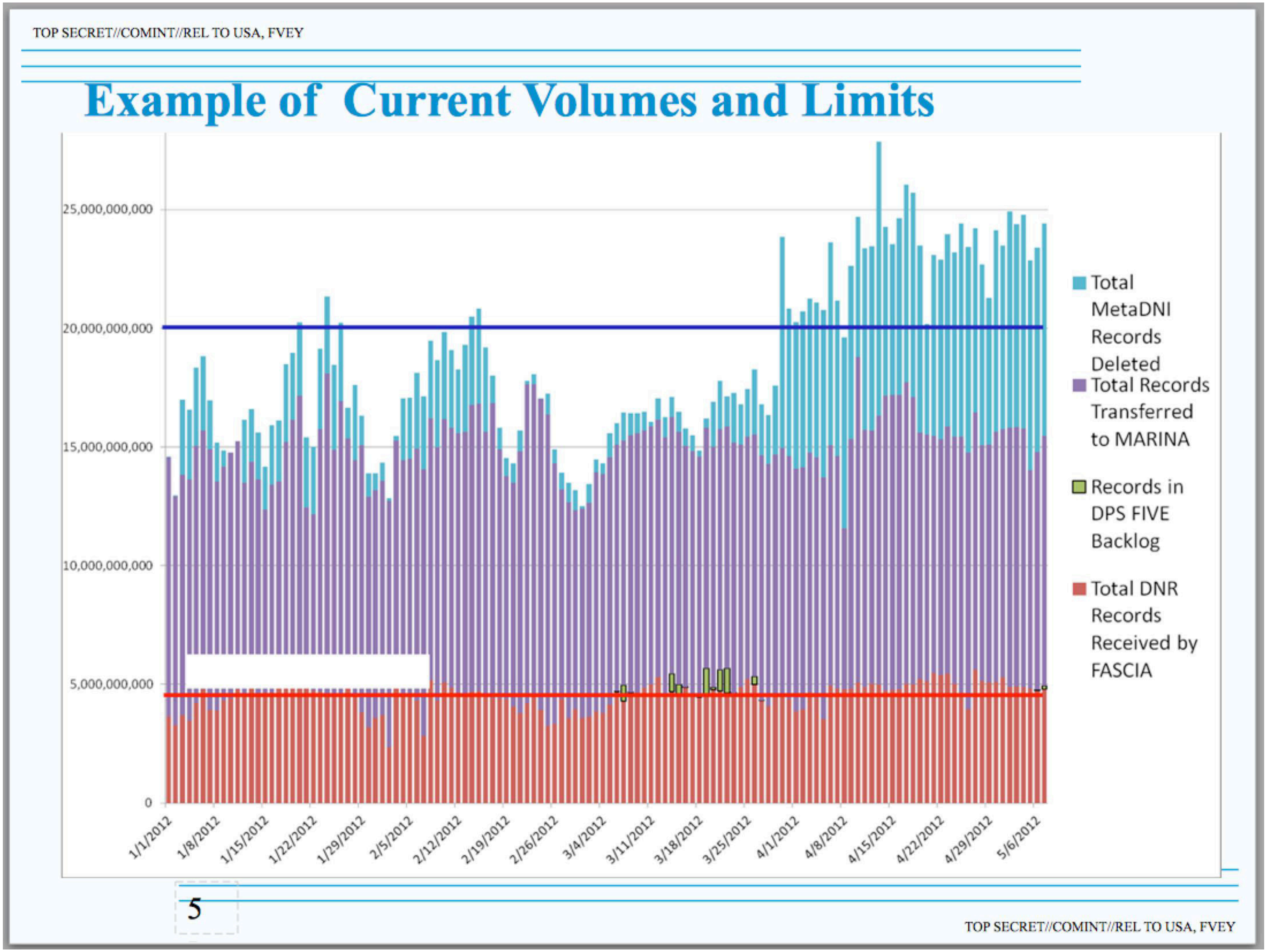
Why TARMAC?

- MHS has a growing FORNSAT mission.
  - SHAREDVISION mission.
  - SigDev ("Difficult Signals collection").
  - ASPHALT ("Collect it All" proof-of-concept system).

Future Plans (U)

(TS//SI//REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

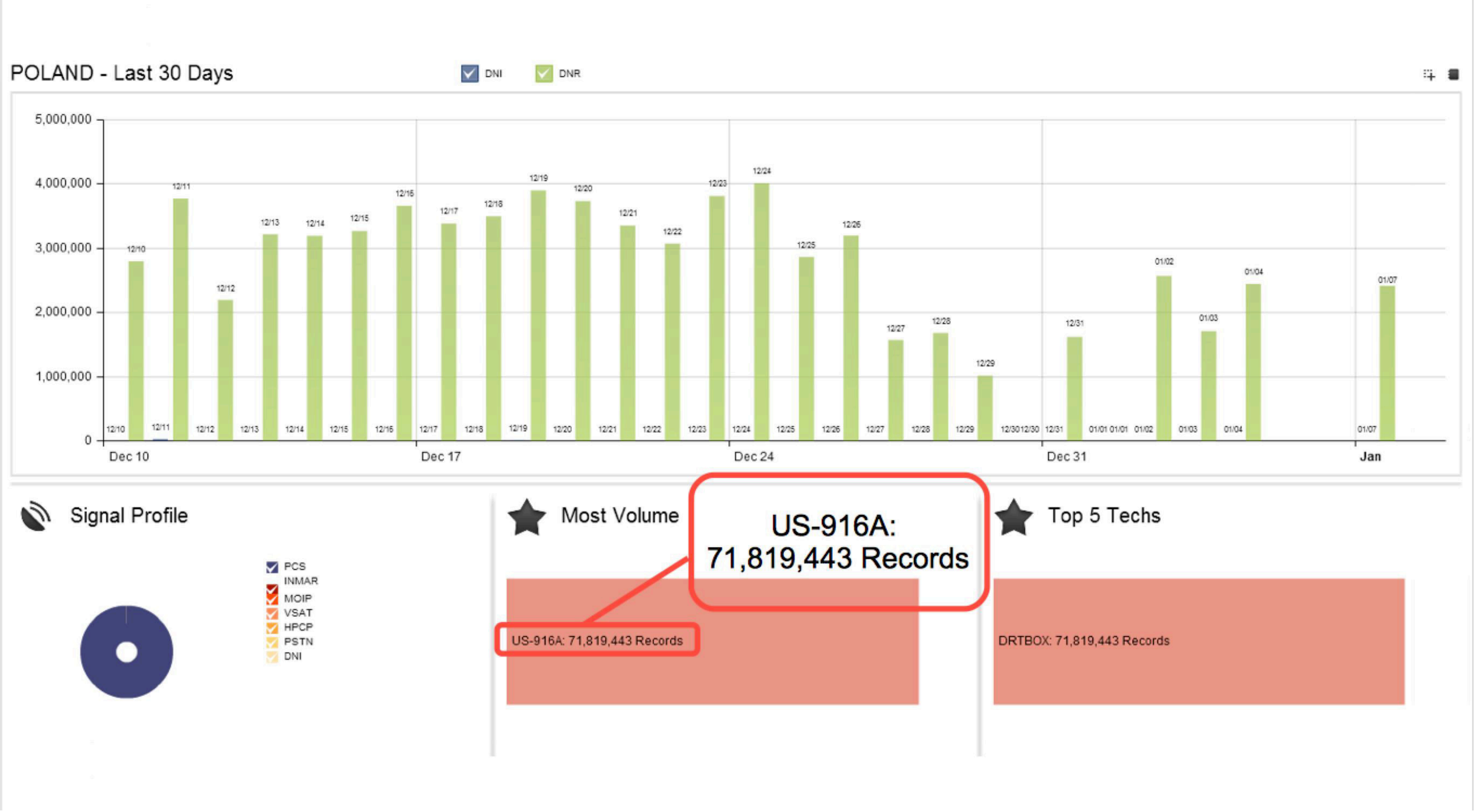


TOP SECRET//COMINT//REL TO USA, FVEY

Example of Current Volumes and Limits

5

TOP SECRET//COMINT//REL TO USA, FVEY



POLAND - Last 30 Days

Signal Profile

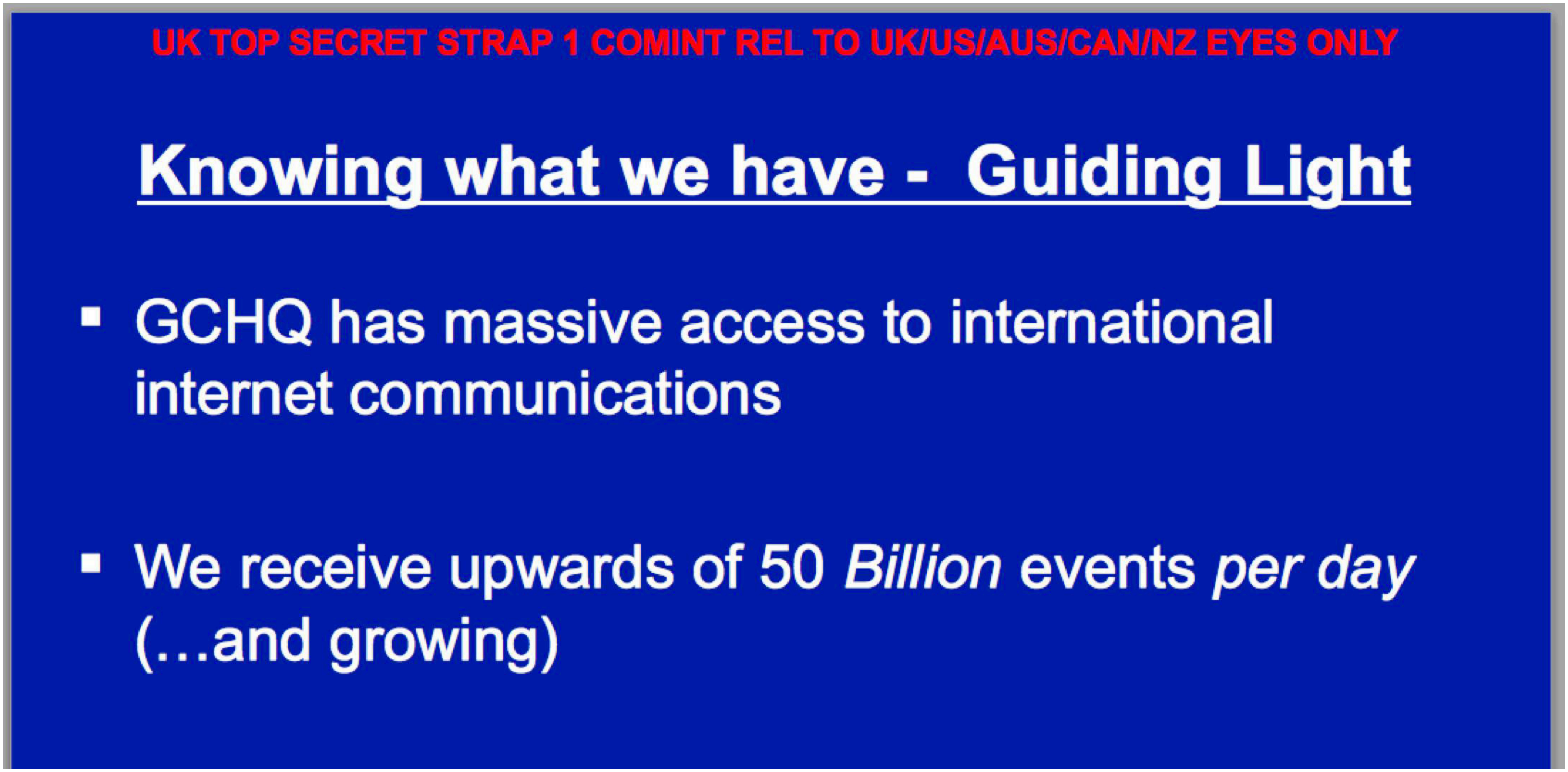
Most Volume

US-916A: 71,819,443 Records

US-916A: 71,819,443 Records

Top 5 Techs

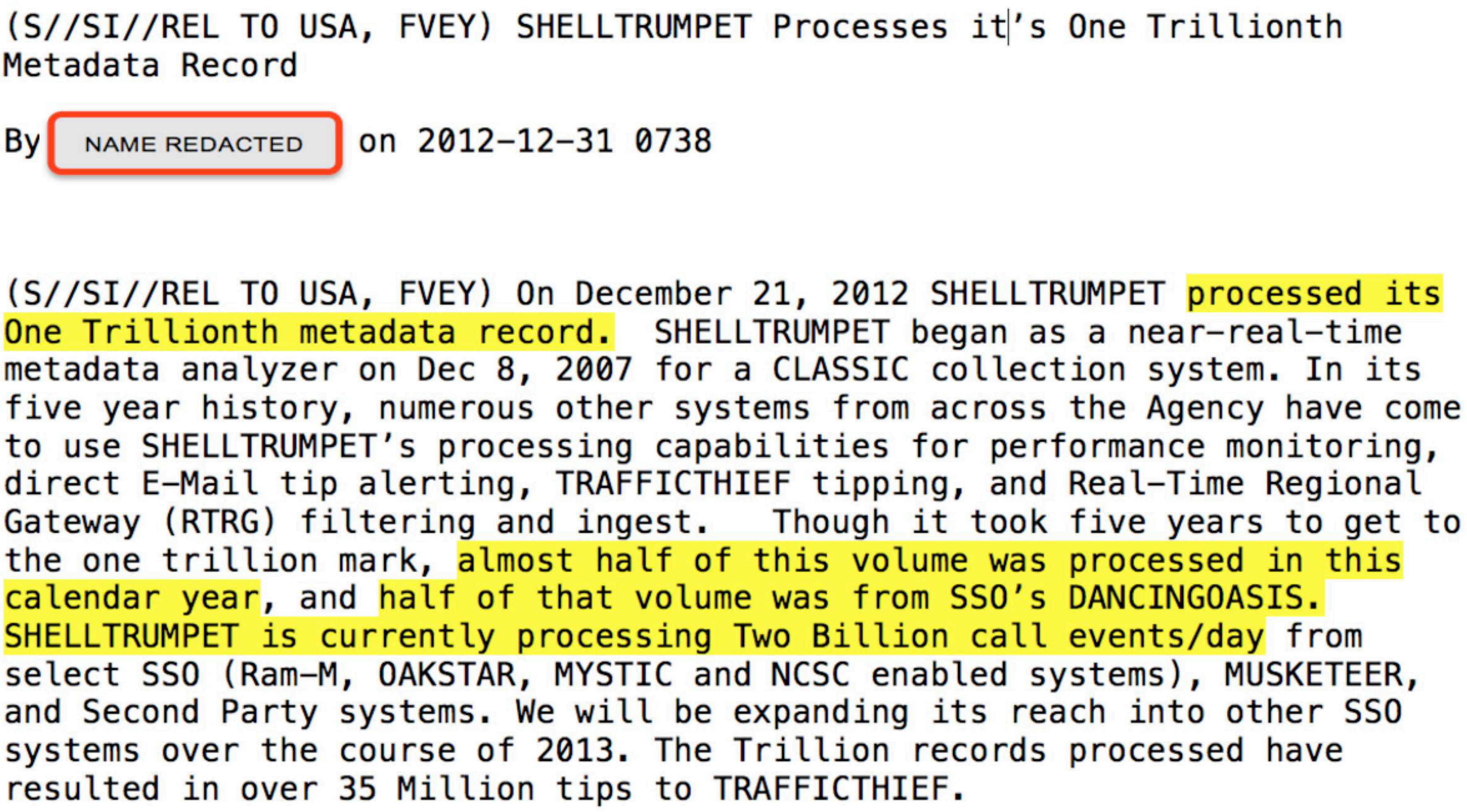
DRTBOX: 71,819,443 Records



UK TOP SECRET STRAP 1 COMINT REL TO UK/US/AUS/CAN/NZ EYES ONLY

Knowing what we have - Guiding Light

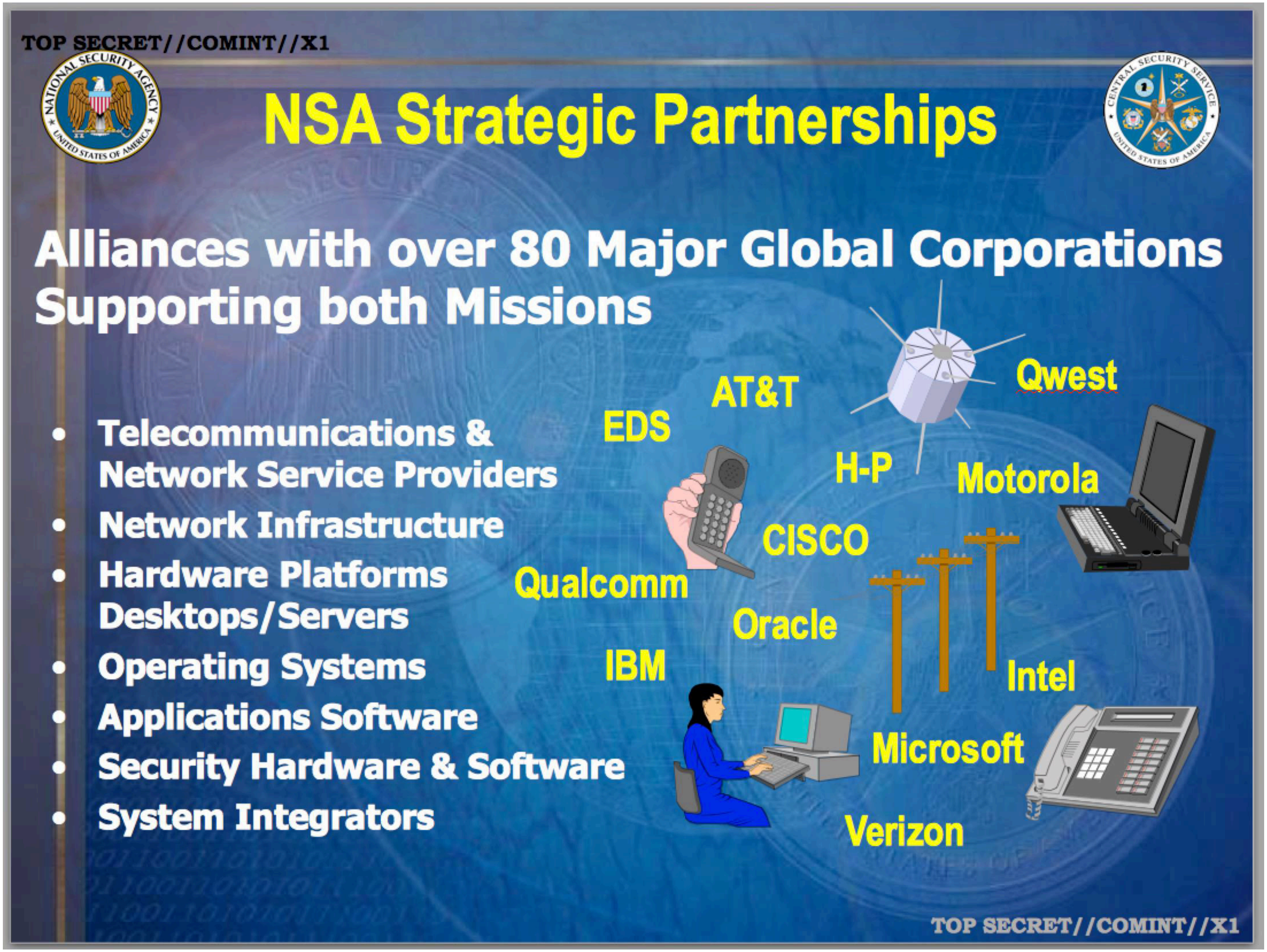
- GCHQ has massive access to international internet communications
- We receive upwards of 50 *Billion* events *per day* (…and growing)



(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes it’s One Trillionth Metadata Record

By NAME REDACTED on 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET’s processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO’s DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETEER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.



TOP SECRET//COMINT//X1

NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

AT&T

Qwest

EDS

H-P

Motorola

CISCO

Qualcomm

Oracle

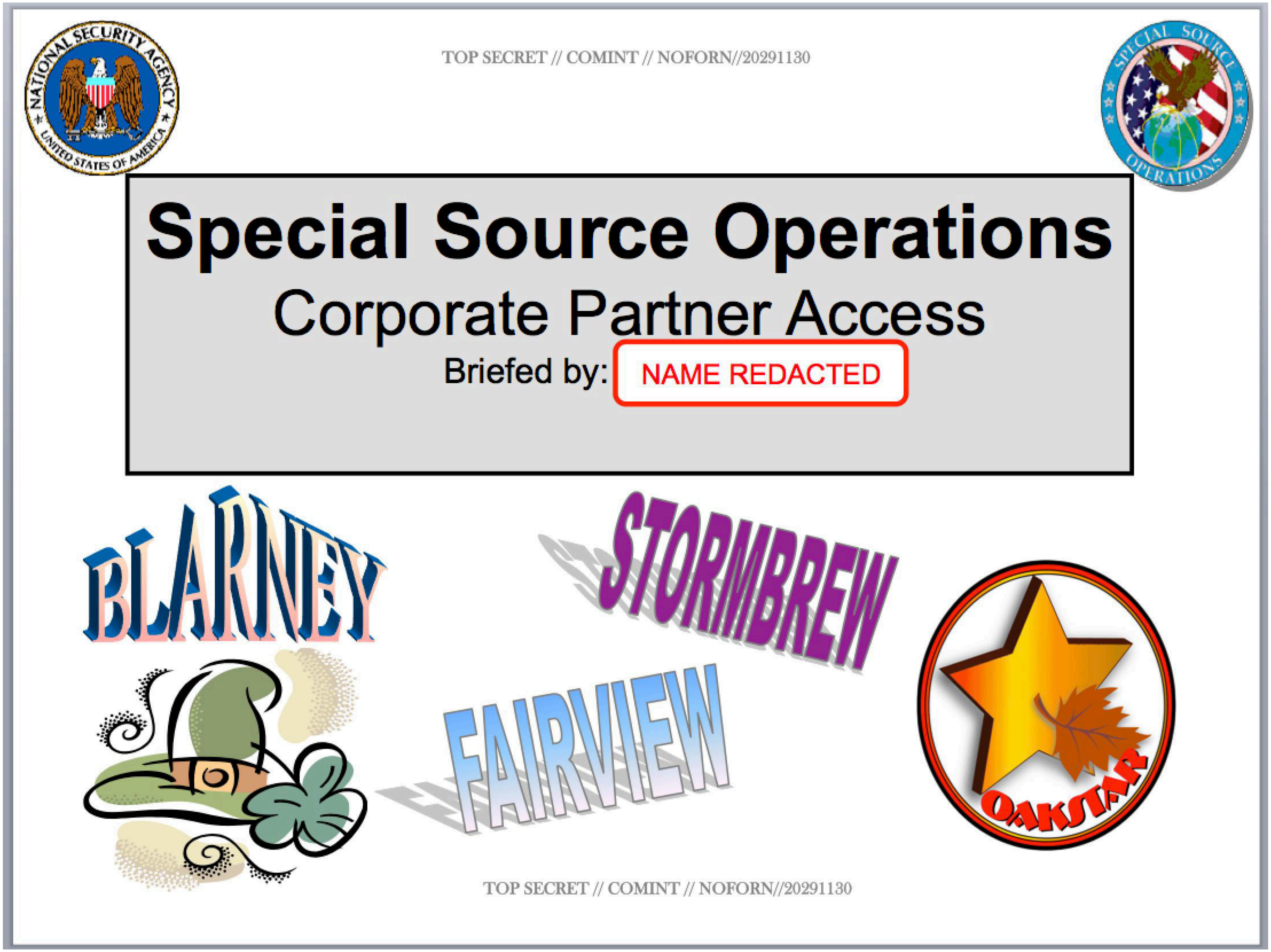
IBM

Intel

Microsoft

Verizon

TOP SECRET//COMINT//X1



TOP SECRET // COMINT // NOFORN//20291130

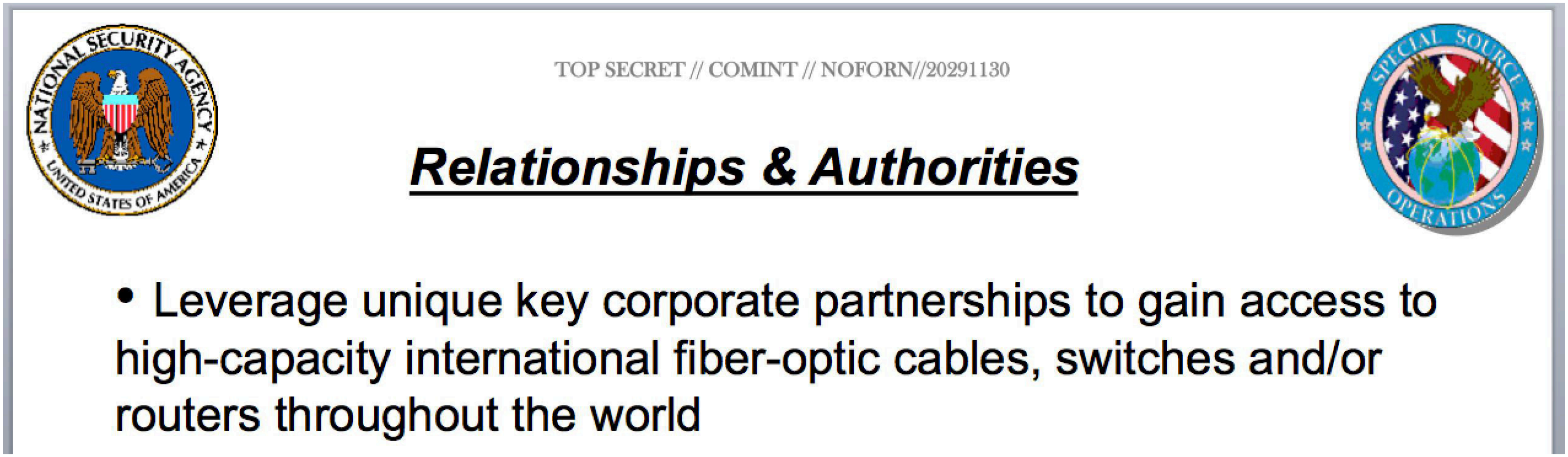
Special Source Operations

Corporate Partner Access

Briefed by: NAME REDACTED

BLARNEY
STORMBREW
FAIRVIEW
OAKSTAR

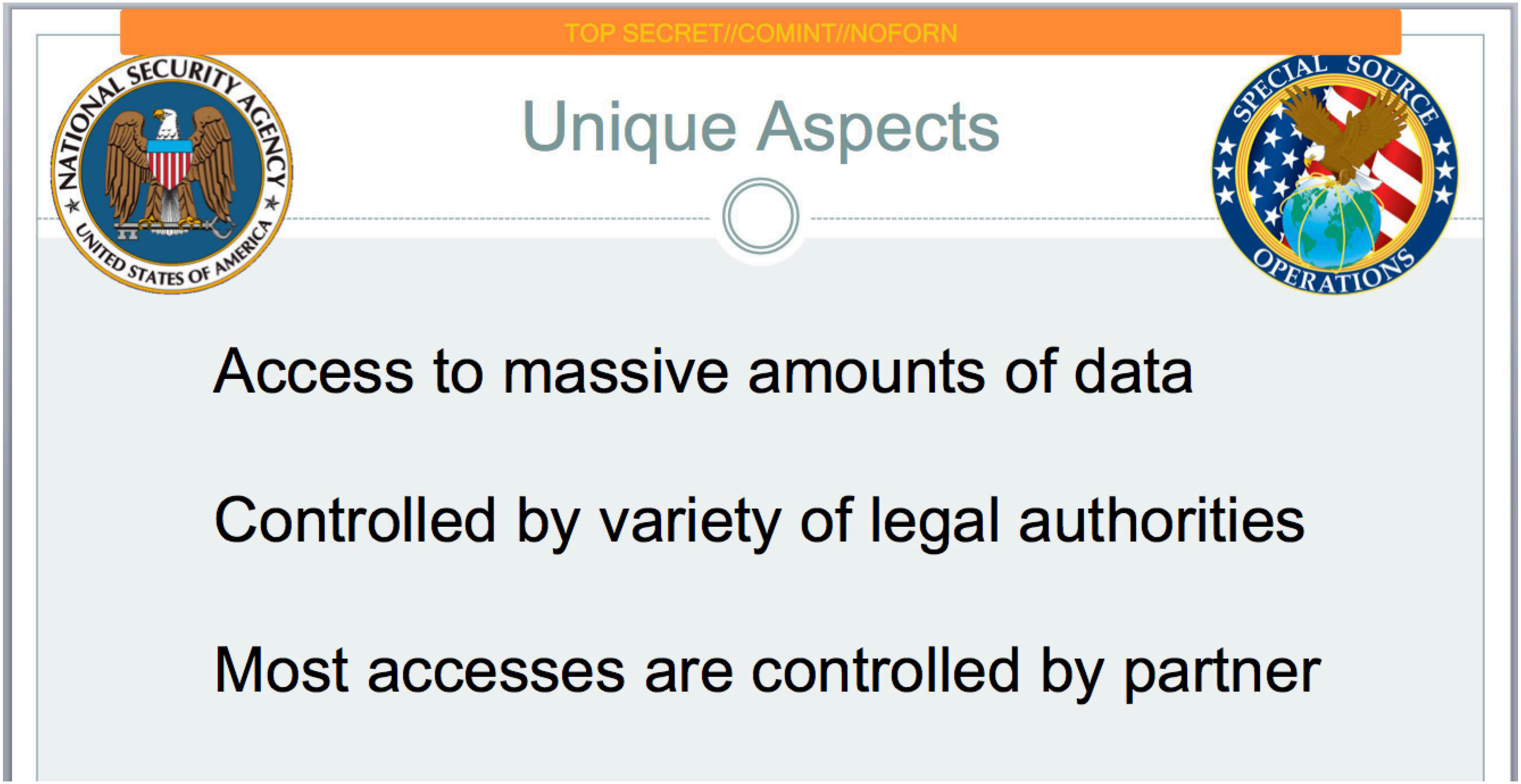
TOP SECRET // COMINT // NOFORN//20291130



TOP SECRET // COMINT // NOFORN//20291130

Relationships & Authorities

- Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world



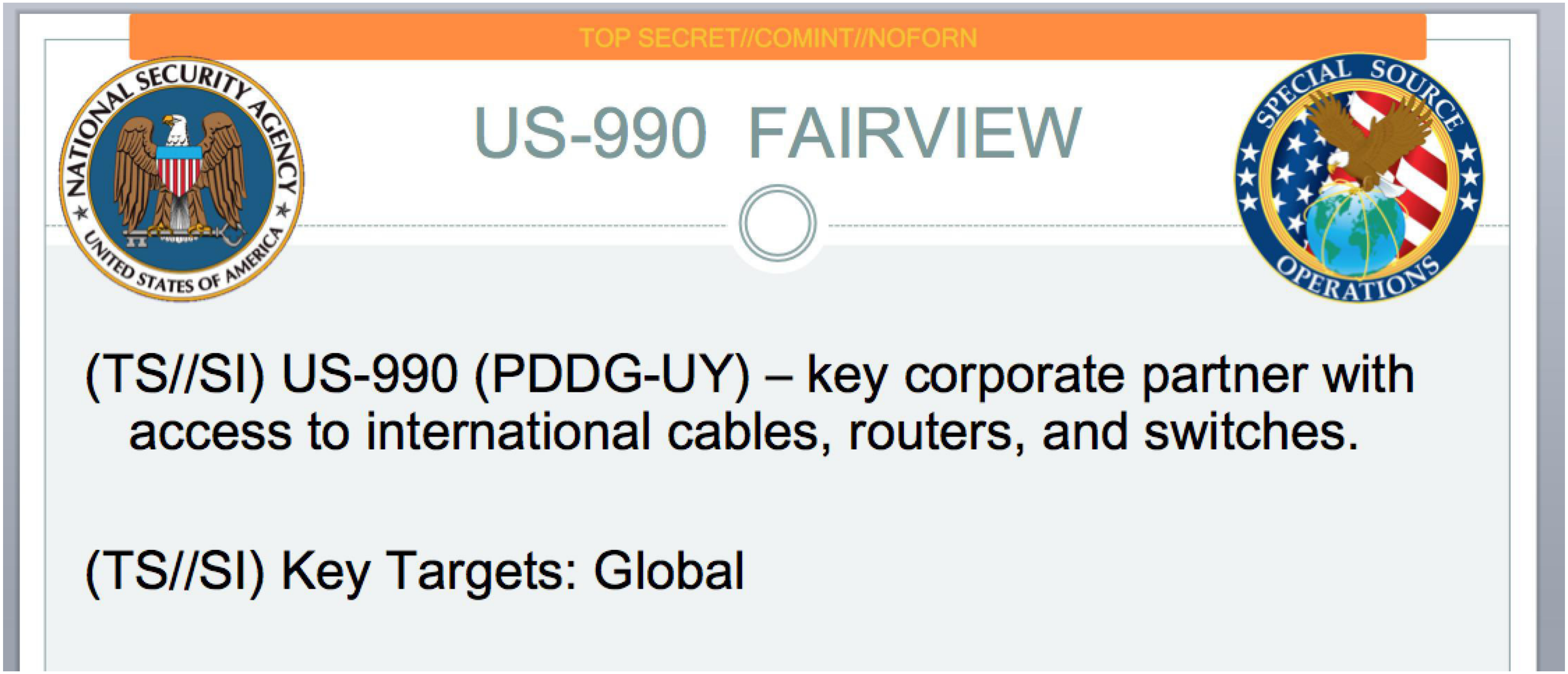
TOP SECRET//COMINT//NOFORN

Unique Aspects

Access to massive amounts of data

Controlled by variety of legal authorities

Most accesses are controlled by partner



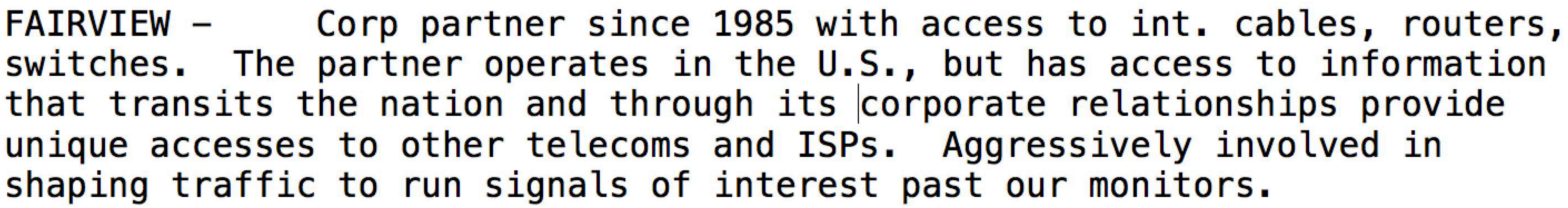
TOP SECRET//COMINT//NOFORN

US-990 FAIRVIEW

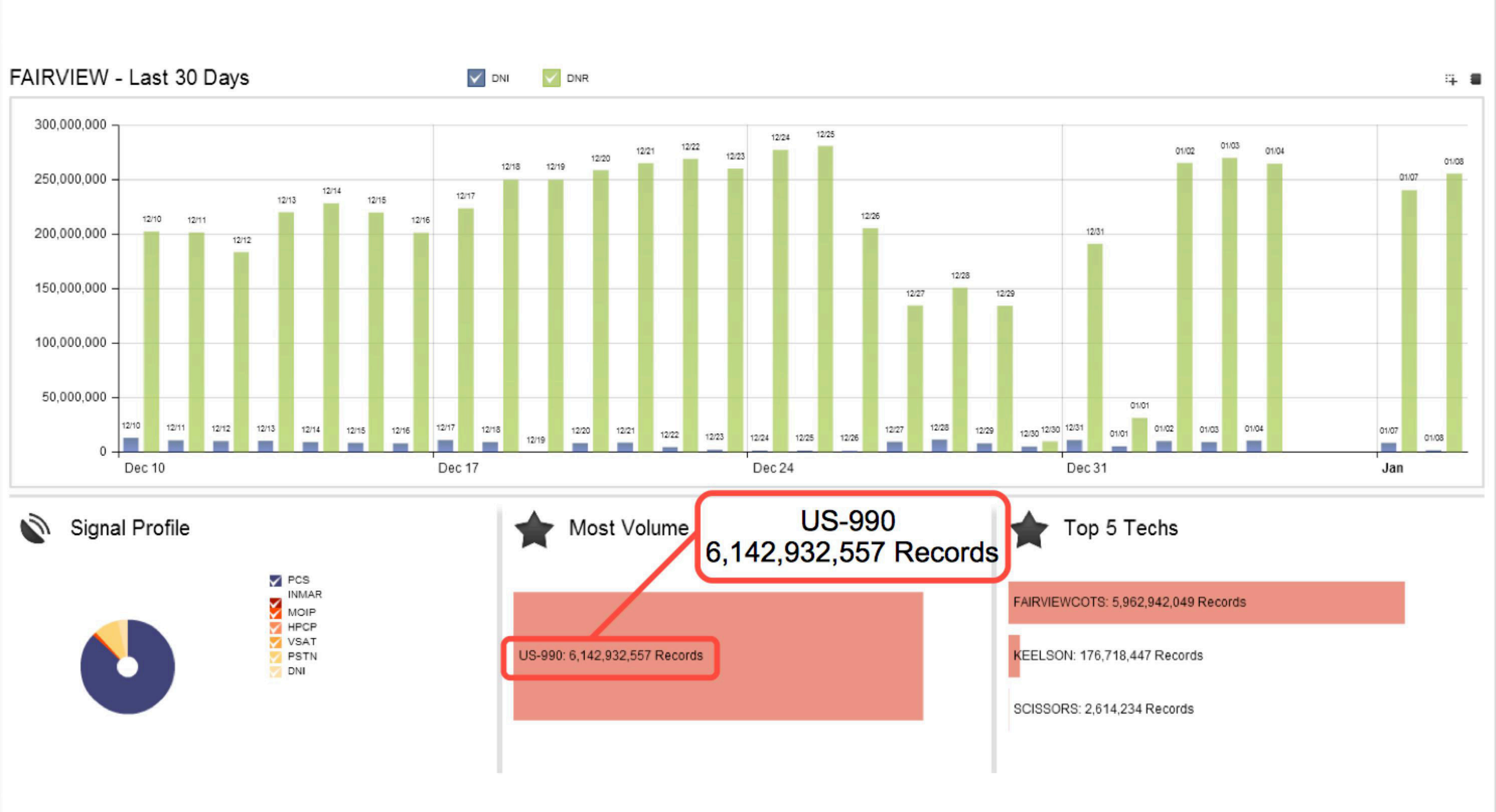
(TS//SI) US-990 (PDDG-UY) – key corporate partner with access to international cables, routers, and switches.

(TS//SI) Key Targets: Global

Page 105



FAIRVIEW – Corp partner since 1985 with access to int. cables, routers, switches. The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs. Aggressively involved in shaping traffic to run signals of interest past our monitors.



FAIRVIEW - Last 30 Days

☑ DNI ☑ DNR

Signal Profile

☑ PCS
INMAR
☑ MOIP
☑ HPCP
☑ VSAT
☑ PSTN
☑ DNI

Most Volume

US-990
6,142,932,557 Records

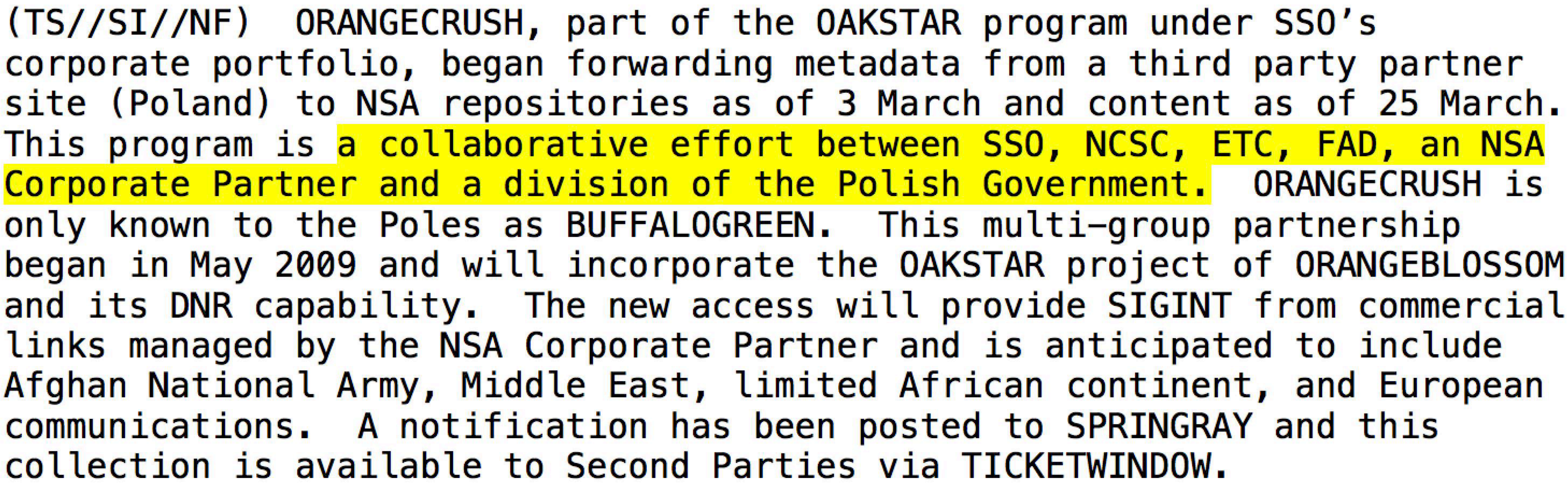
US-990: 6,142,932,557 Records

Top 5 Techs

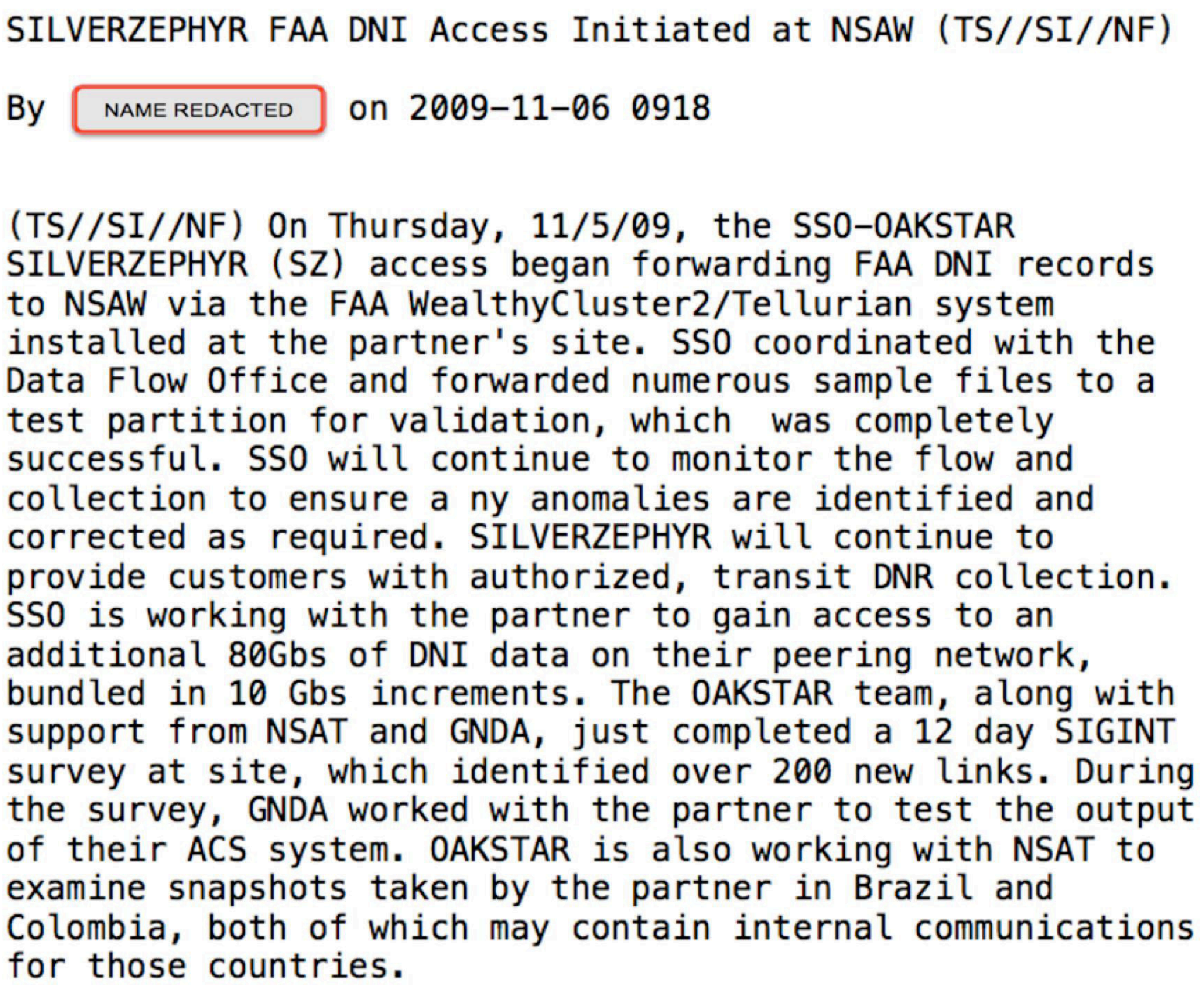
FAIRVIEWCOTS: 5,962,942,049 Records

KEELSON: 176,718,447 Records

SCISSORS: 2,614,234 Records



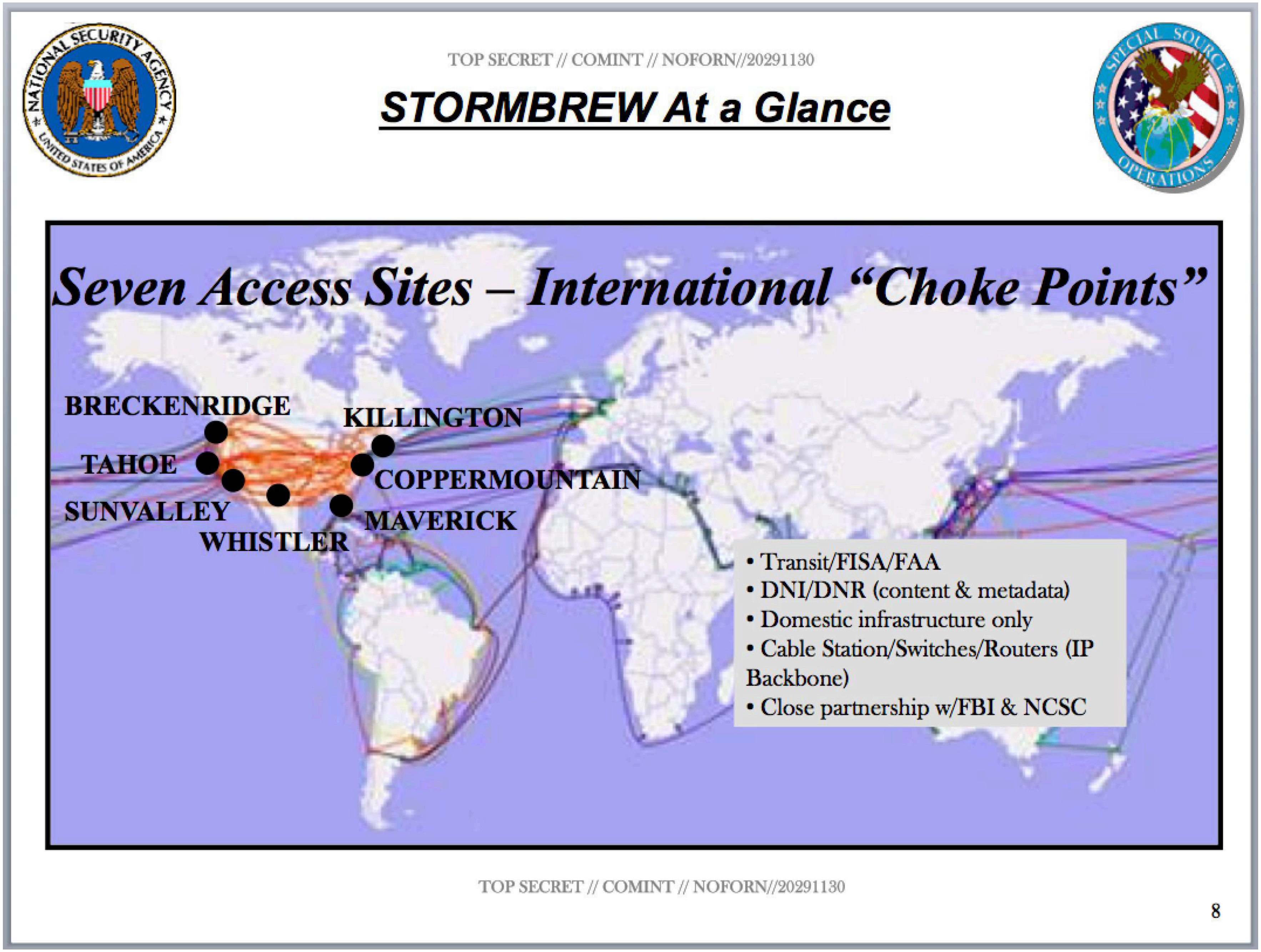
(TS//SI//NF) ORANGECRUSH, part of the OAKSTAR program under SSO's corporate portfolio, began forwarding metadata from a third party partner site (Poland) to NSA repositories as of 3 March and content as of 25 March. This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA Corporate Partner and a division of the Polish Government. ORANGECRUSH is only known to the Poles as BUFFALOGREEN. This multi-group partnership began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM and its DNR capability. The new access will provide SIGINT from commercial links managed by the NSA Corporate Partner and is anticipated to include Afghan National Army, Middle East, limited African continent, and European communications. A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW.



SILVERZEPHYR FAA DNI Access Initiated at NSAW (TS//SI//NF)

By NAME REDACTED on 2009-11-06 0918

(TS//SI//NF) On Thursday, 11/5/09, the SSO-OAKSTAR SILVERZEPHYR (SZ) access began forwarding FAA DNI records to NSAW via the FAA WealthyCluster2/Tellurian system installed at the partner's site. SSO coordinated with the Data Flow Office and forwarded numerous sample files to a test partition for validation, which was completely successful. SSO will continue to monitor the flow and collection to ensure a ny anomalies are identified and corrected as required. SILVERZEPHYR will continue to provide customers with authorized, transit DNR collection. SSO is working with the partner to gain access to an additional 80Gbs of DNI data on their peering network, bundled in 10 Gbs increments. The OAKSTAR team, along with support from NSAT and GNDA, just completed a 12 day SIGINT survey at site, which identified over 200 new links. During the survey, GNDA worked with the partner to test the output of their ACS system. OAKSTAR is also working with NSAT to examine snapshots taken by the partner in Brazil and Colombia, both of which may contain internal communications for those countries.

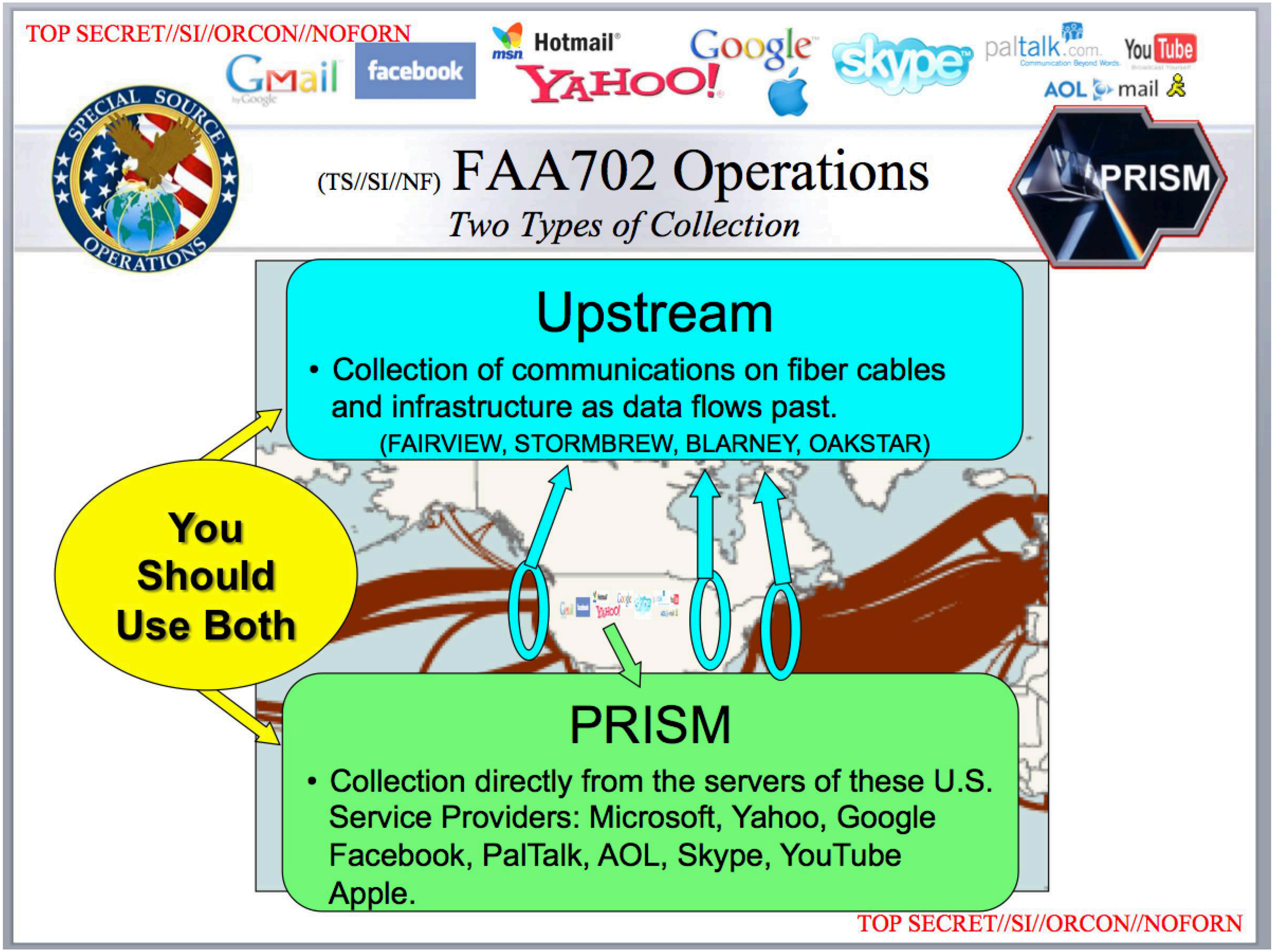


STORMBREW At a Glance

Seven Access Sites – International "Choke Points"

- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Station/Switches/Routers (IP Backbone)
- Close partnership w/FBI & NCSC

Page 108



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

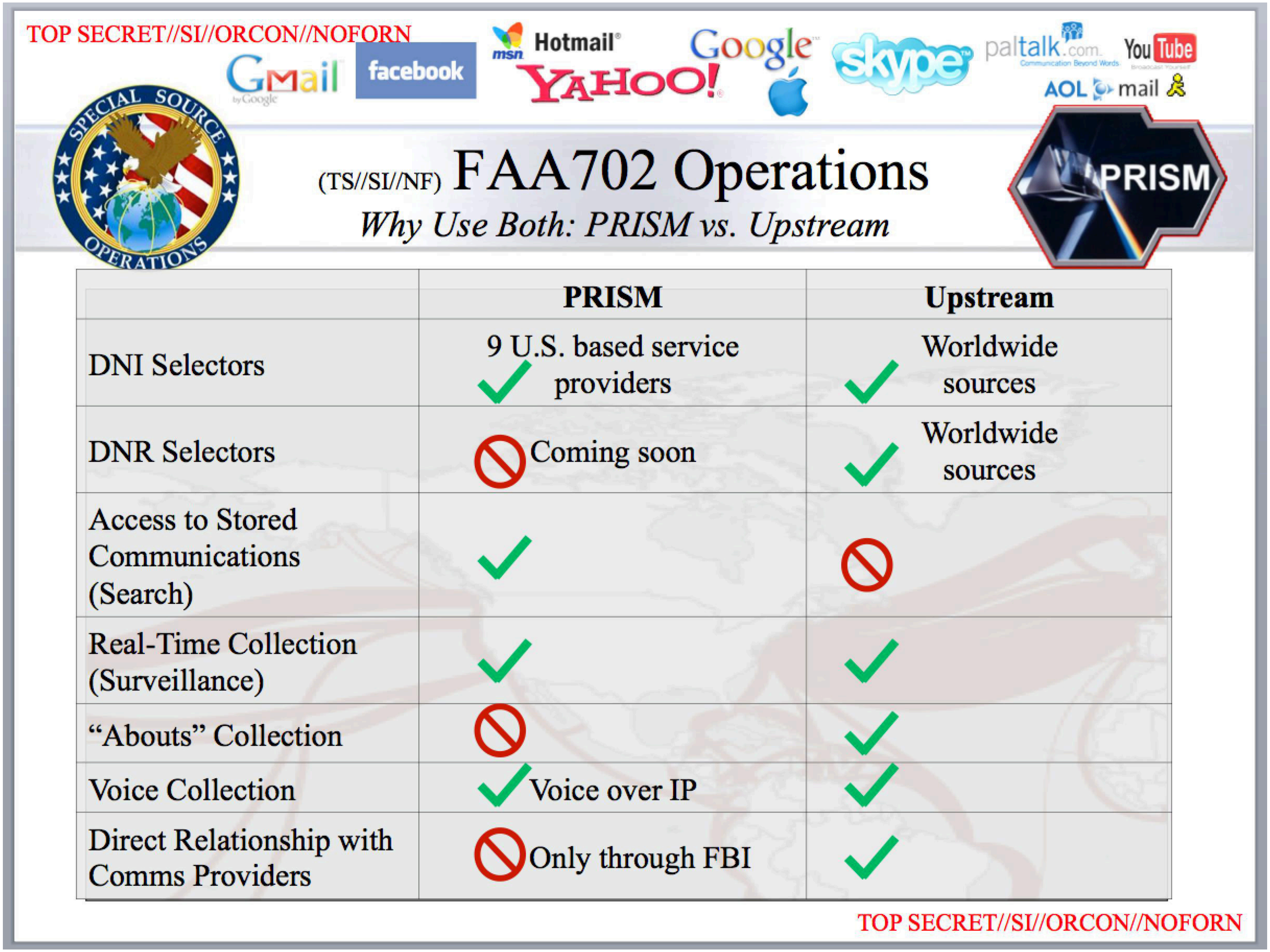
(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN


GMail by Google
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com Communication Beyond Words
YouTube Broadcast Yourself
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

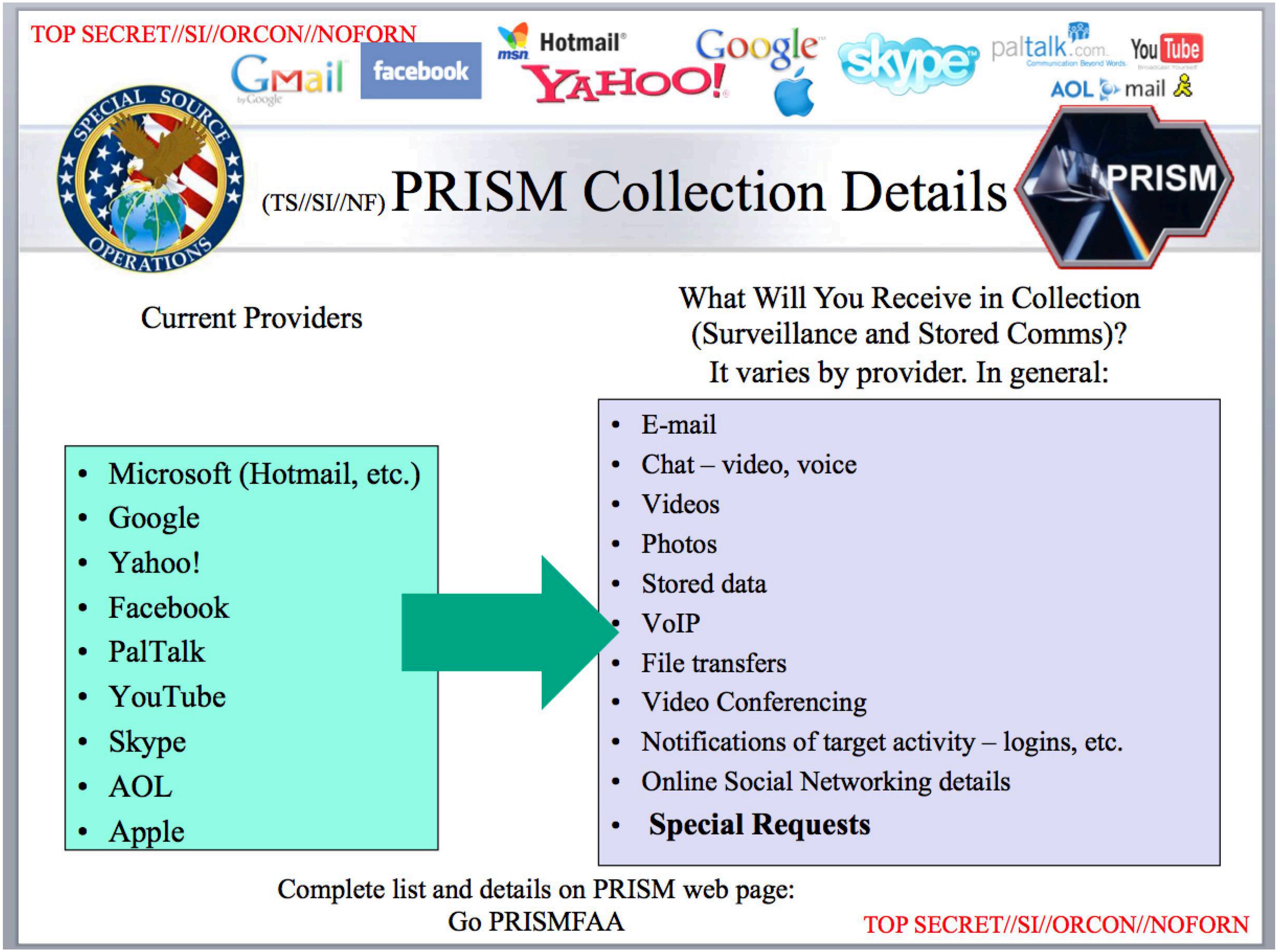
TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	✓ 9 U.S. based service providers	✓ Worldwide sources
DNR Selectors	⊘ Coming soon	✓ Worldwide sources
Access to Stored Communications (Search)	✓	⊘
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	⊘	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	⊘ Only through FBI	✓

TOP SECRET//SI//ORCON//NOFORN



GMail by Google
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com Communication Beyond Words
YouTube Broadcast Yourself
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

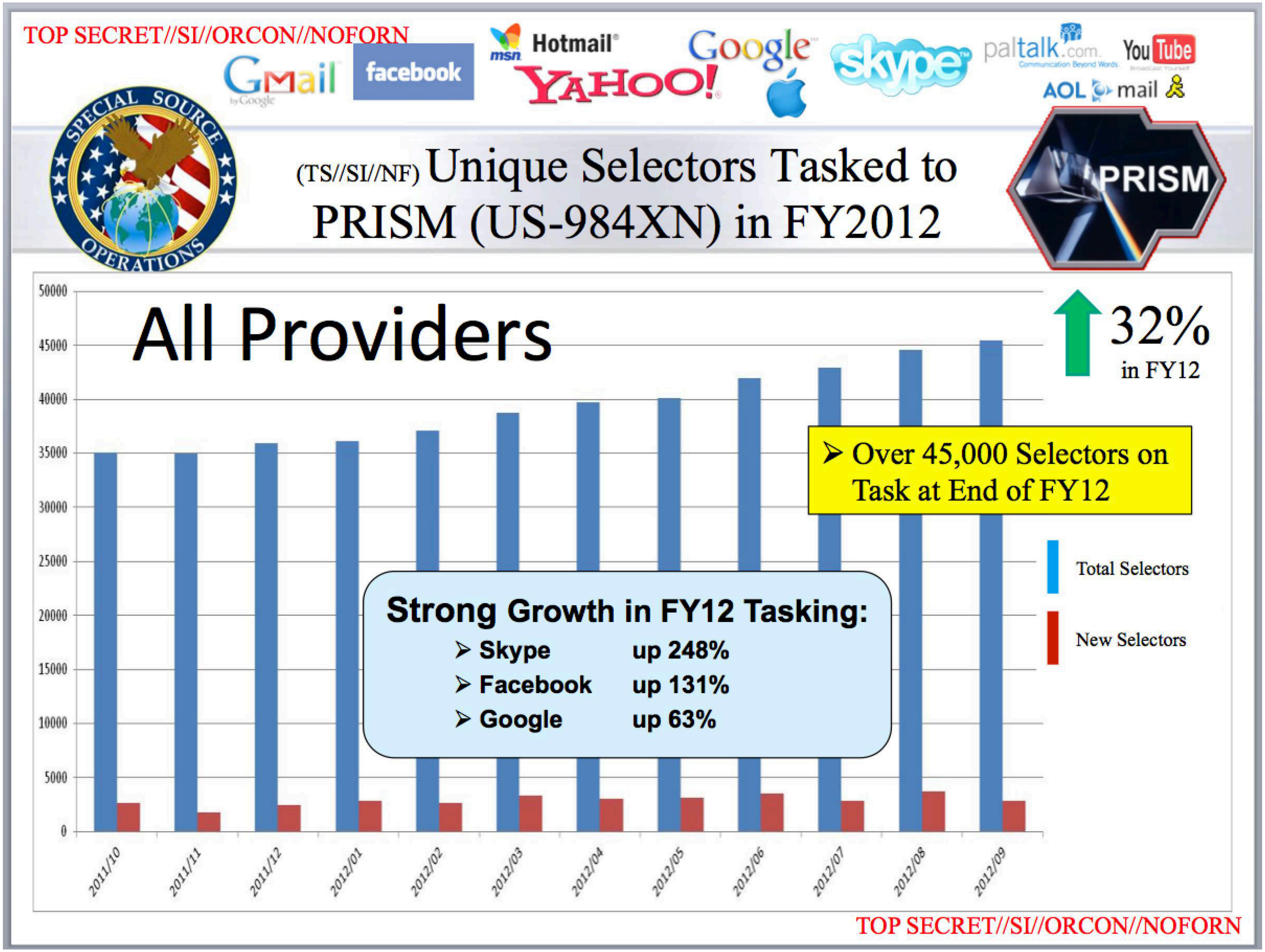
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection
(Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Unique Selectors Tasked to PRISM (US-984XN) in FY2012

All Providers

32% in FY12

➢ Over 45,000 Selectors on Task at End of FY12

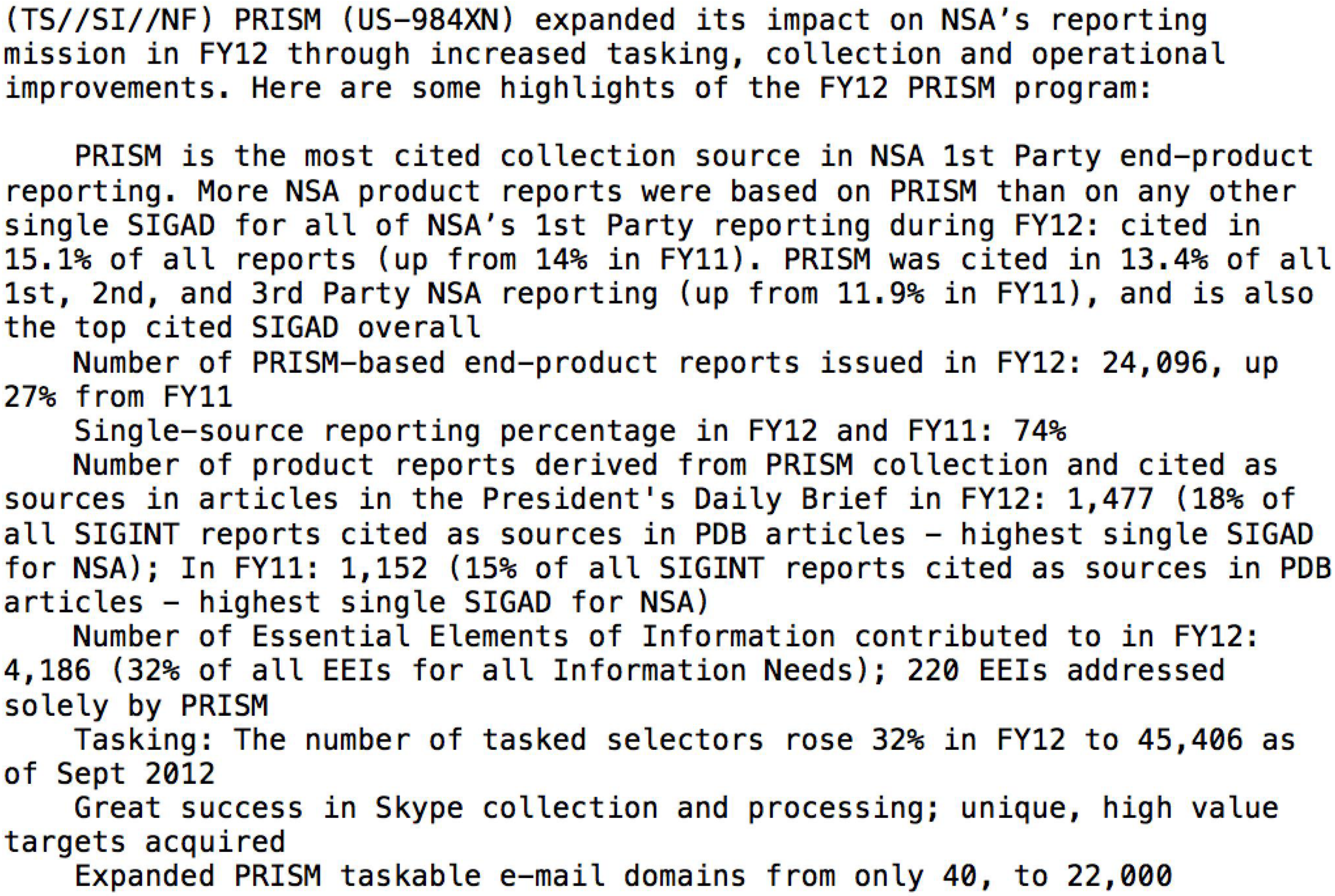
Strong Growth in FY12 Tasking:

➢ Skype	up 248%
➢ Facebook	up 131%
➢ Google	up 63%

Total Selectors

New Selectors

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) PRISM (US-984XN) expanded its impact on NSA’s reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:

PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA’s 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall

Number of PRISM-based end-product reports issued in FY12: 24,096, up 27% from FY11

Single-source reporting percentage in FY12 and FY11: 74%

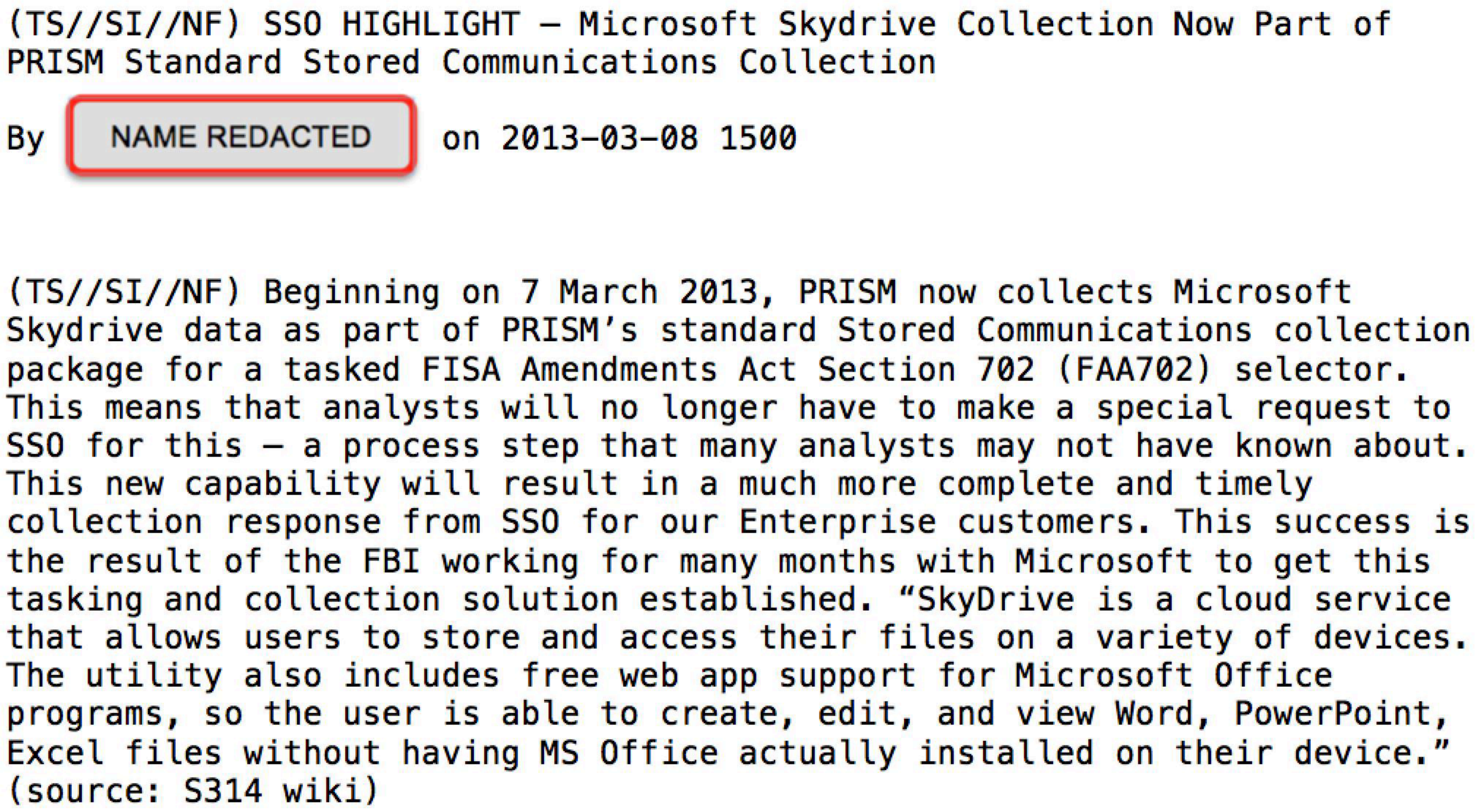
Number of product reports derived from PRISM collection and cited as sources in articles in the President's Daily Brief in FY12: 1,477 (18% of all SIGINT reports cited as sources in PDB articles – highest single SIGAD for NSA); In FY11: 1,152 (15% of all SIGINT reports cited as sources in PDB articles – highest single SIGAD for NSA)

Number of Essential Elements of Information contributed to in FY12: 4,186 (32% of all EEIs for all Information Needs); 220 EEIs addressed solely by PRISM

Tasking: The number of tasked selectors rose 32% in FY12 to 45,406 as of Sept 2012

Great success in Skype collection and processing; unique, high value targets acquired

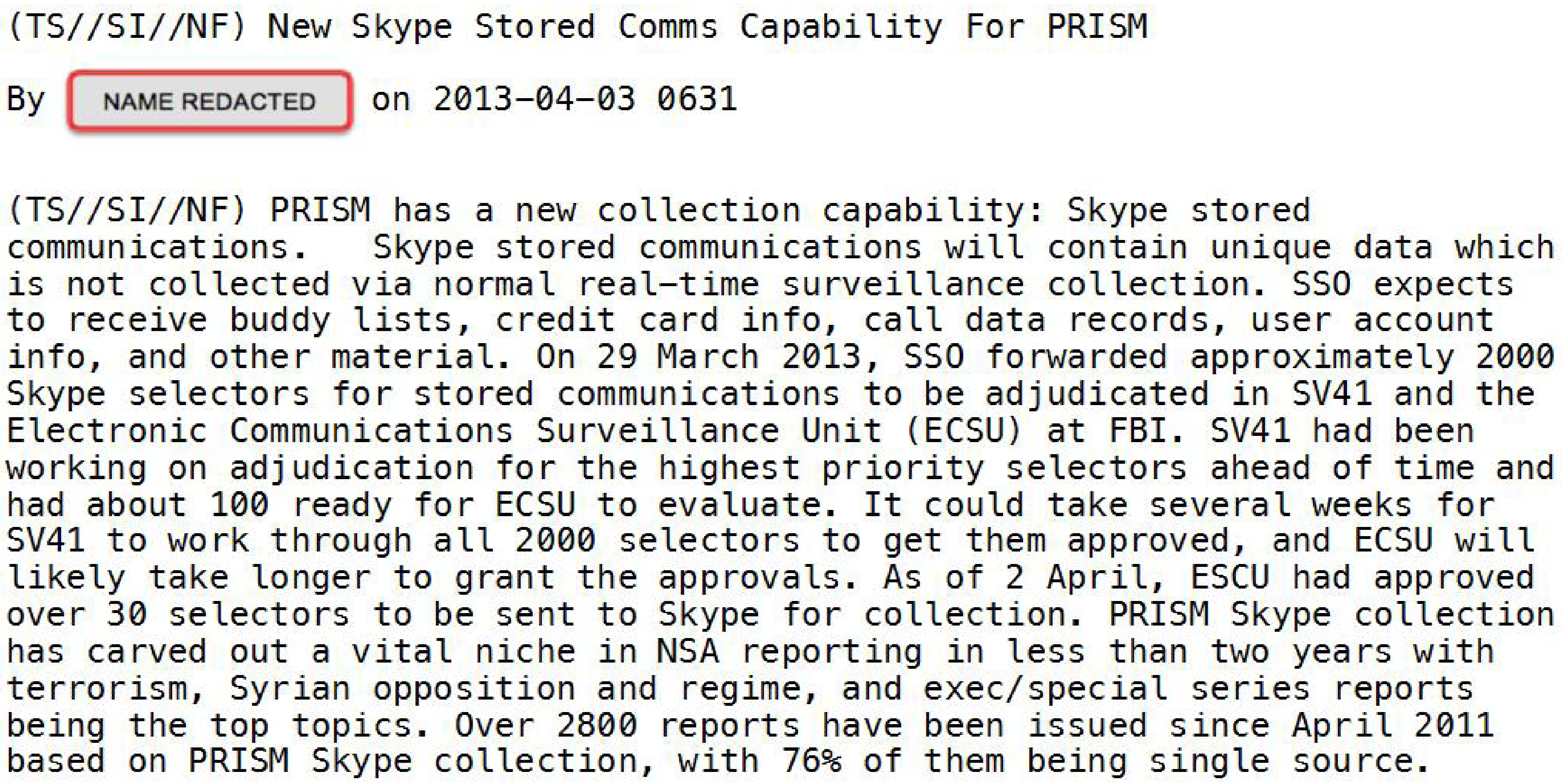
Expanded PRISM taskable e-mail domains from only 40, to 22,000



(TS//SI//NF) SSO HIGHLIGHT – Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection

By NAME REDACTED on 2013-03-08 1500

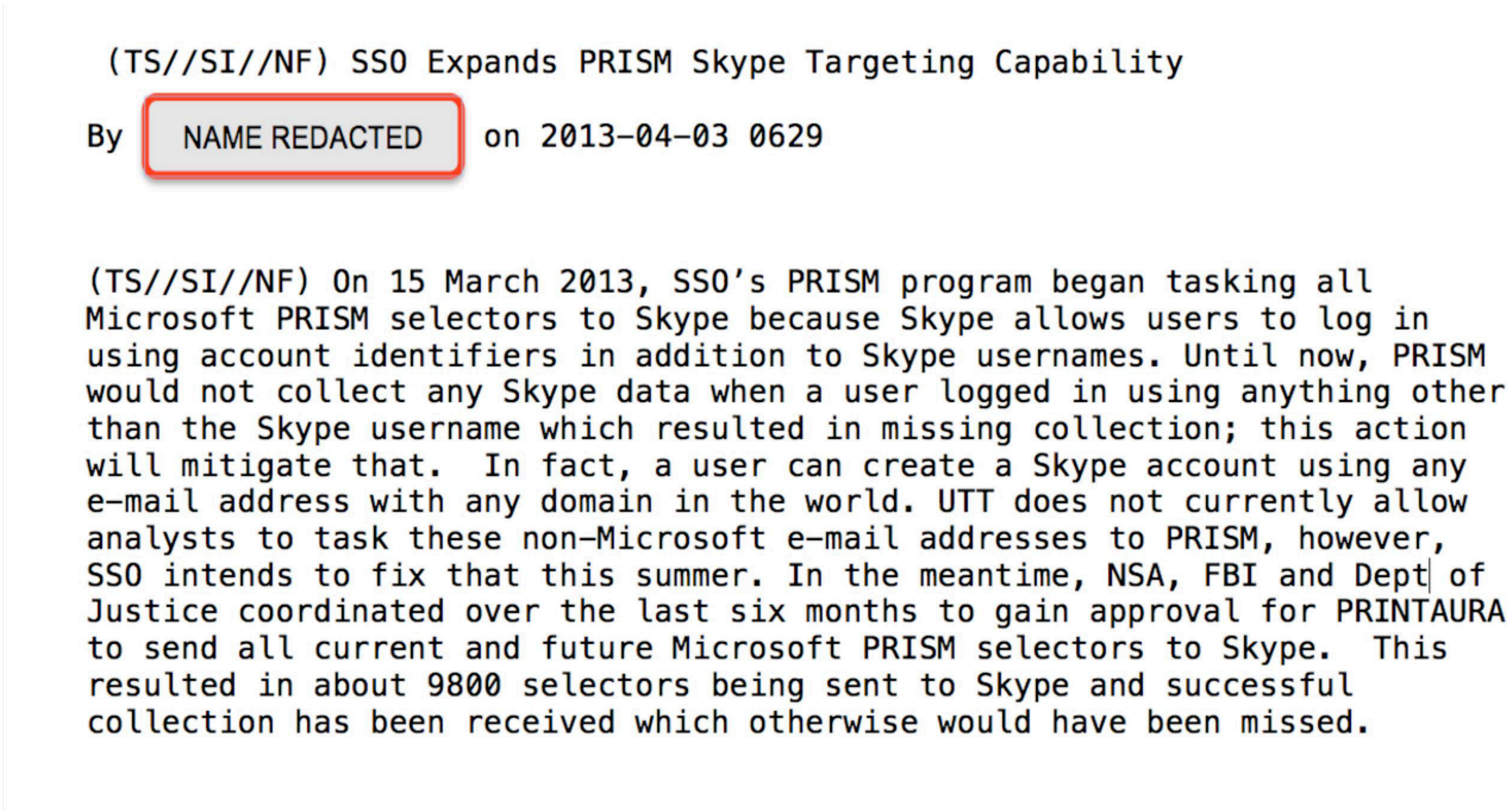
(TS//SI//NF) Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package for a tasked FISA Amendments Act Section 702 (FAA702) selector. This means that analysts will no longer have to make a special request to SSO for this – a process step that many analysts may not have known about. This new capability will result in a much more complete and timely collection response from SSO for our Enterprise customers. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "SkyDrive is a cloud service that allows users to store and access their files on a variety of devices. The utility also includes free web app support for Microsoft Office programs, so the user is able to create, edit, and view Word, PowerPoint, Excel files without having MS Office actually installed on their device." (source: S314 wiki)



(TS//SI//NF) New Skype Stored Comms Capability For PRISM

By NAME REDACTED on 2013-04-03 0631

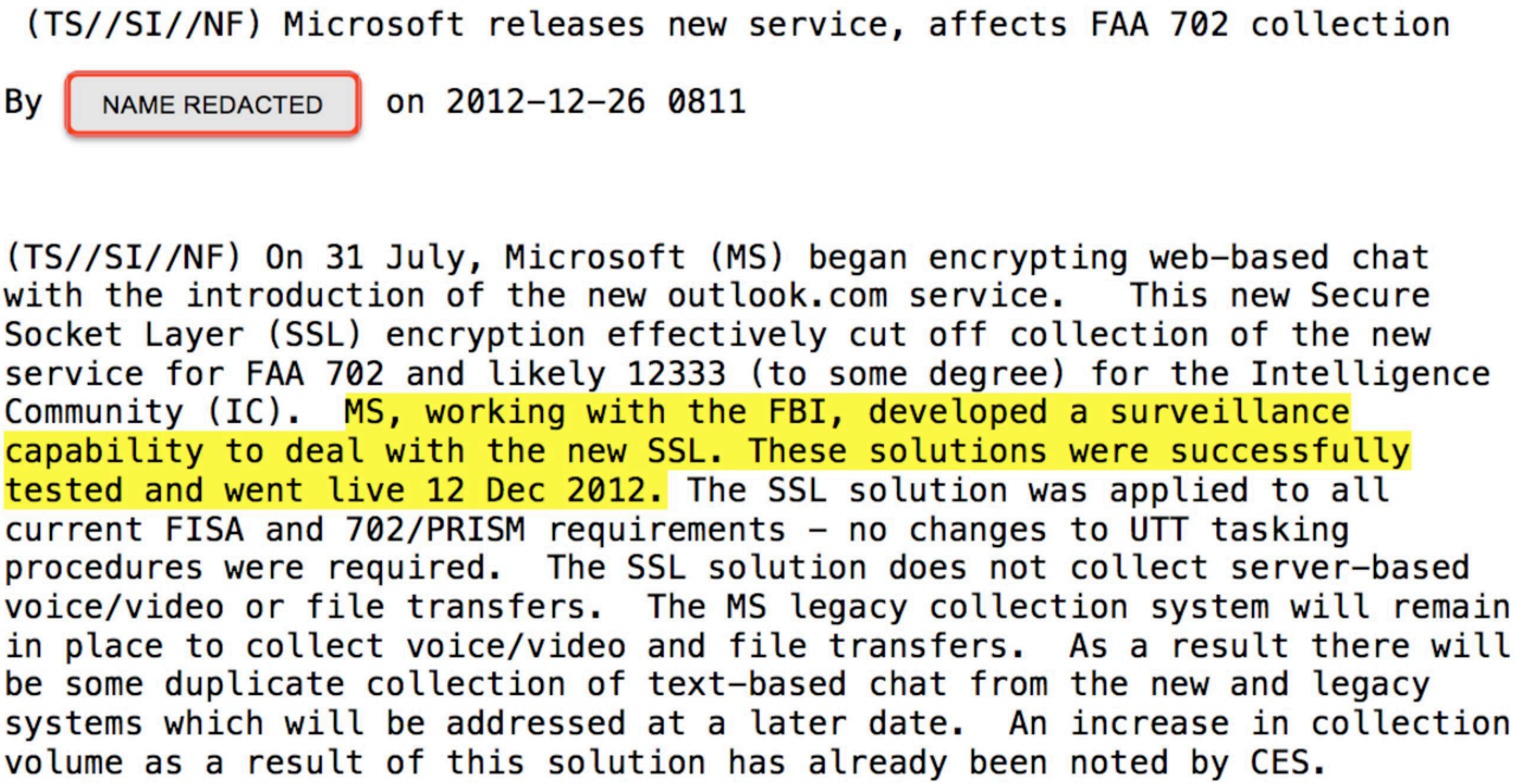
(TS//SI//NF) PRISM has a new collection capability: Skype stored communications. Skype stored communications will contain unique data which is not collected via normal real-time surveillance collection. SSO expects to receive buddy lists, credit card info, call data records, user account info, and other material. On 29 March 2013, SSO forwarded approximately 2000 Skype selectors for stored communications to be adjudicated in SV41 and the Electronic Communications Surveillance Unit (ECSU) at FBI. SV41 had been working on adjudication for the highest priority selectors ahead of time and had about 100 ready for ECSU to evaluate. It could take several weeks for SV41 to work through all 2000 selectors to get them approved, and ECSU will likely take longer to grant the approvals. As of 2 April, ESCU had approved over 30 selectors to be sent to Skype for collection. PRISM Skype collection has carved out a vital niche in NSA reporting in less than two years with terrorism, Syrian opposition and regime, and exec/special series reports being the top topics. Over 2800 reports have been issued since April 2011 based on PRISM Skype collection, with 76% of them being single source.



(TS//SI//NF) SSO Expands PRISM Skype Targeting Capability

By NAME REDACTED on 2013-04-03 0629

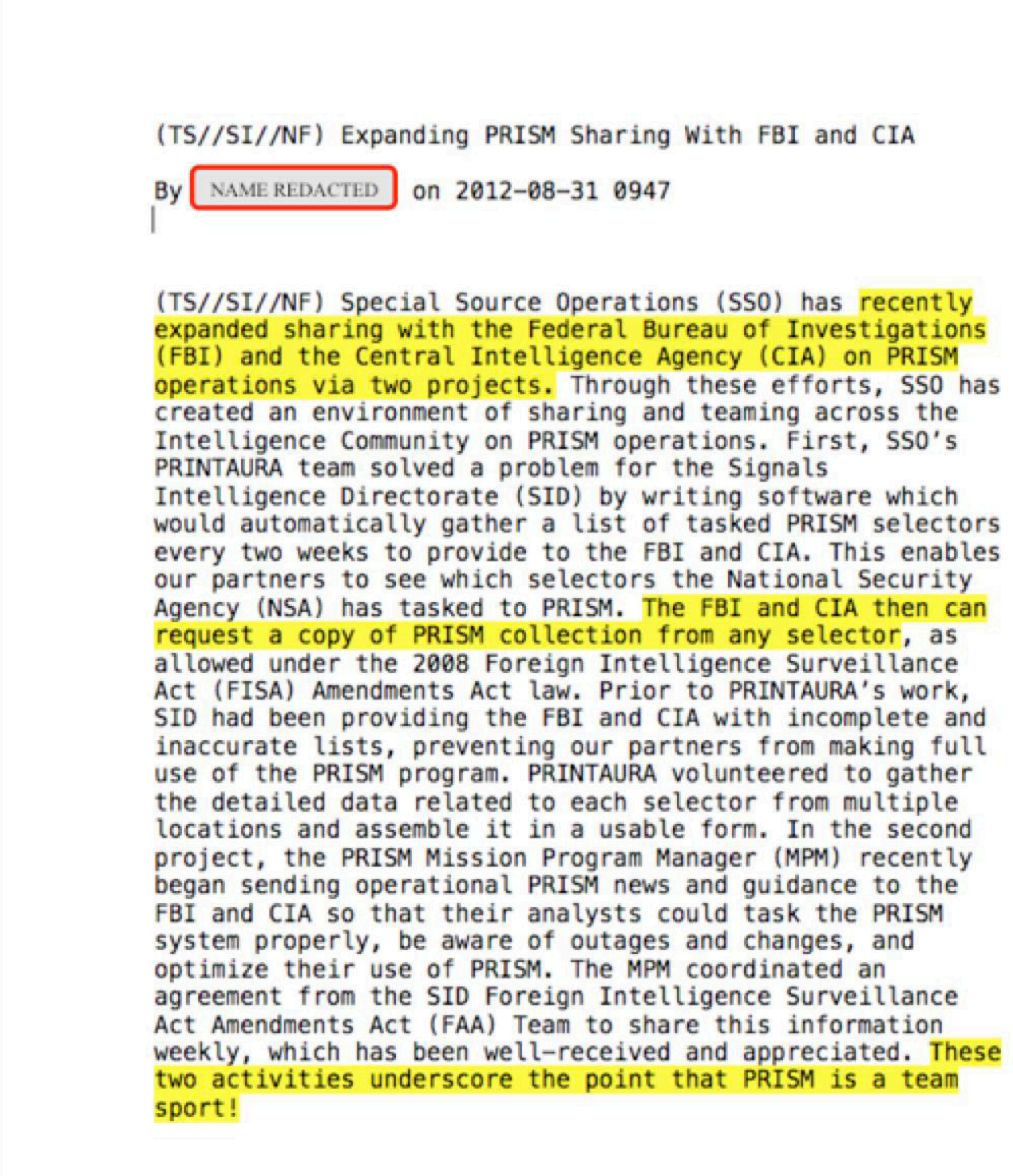
(TS//SI//NF) On 15 March 2013, SSO's PRISM program began tasking all Microsoft PRISM selectors to Skype because Skype allows users to log in using account identifiers in addition to Skype usernames. Until now, PRISM would not collect any Skype data when a user logged in using anything other than the Skype username which resulted in missing collection; this action will mitigate that. In fact, a user can create a Skype account using any e-mail address with any domain in the world. UTT does not currently allow analysts to task these non-Microsoft e-mail addresses to PRISM, however, SSO intends to fix that this summer. In the meantime, NSA, FBI and Dept of Justice coordinated over the last six months to gain approval for PRINTAURA to send all current and future Microsoft PRISM selectors to Skype. This resulted in about 9800 selectors being sent to Skype and successful collection has been received which otherwise would have been missed.



(TS//SI//NF) Microsoft releases new service, affects FAA 702 collection

By NAME REDACTED on 2012-12-26 0811

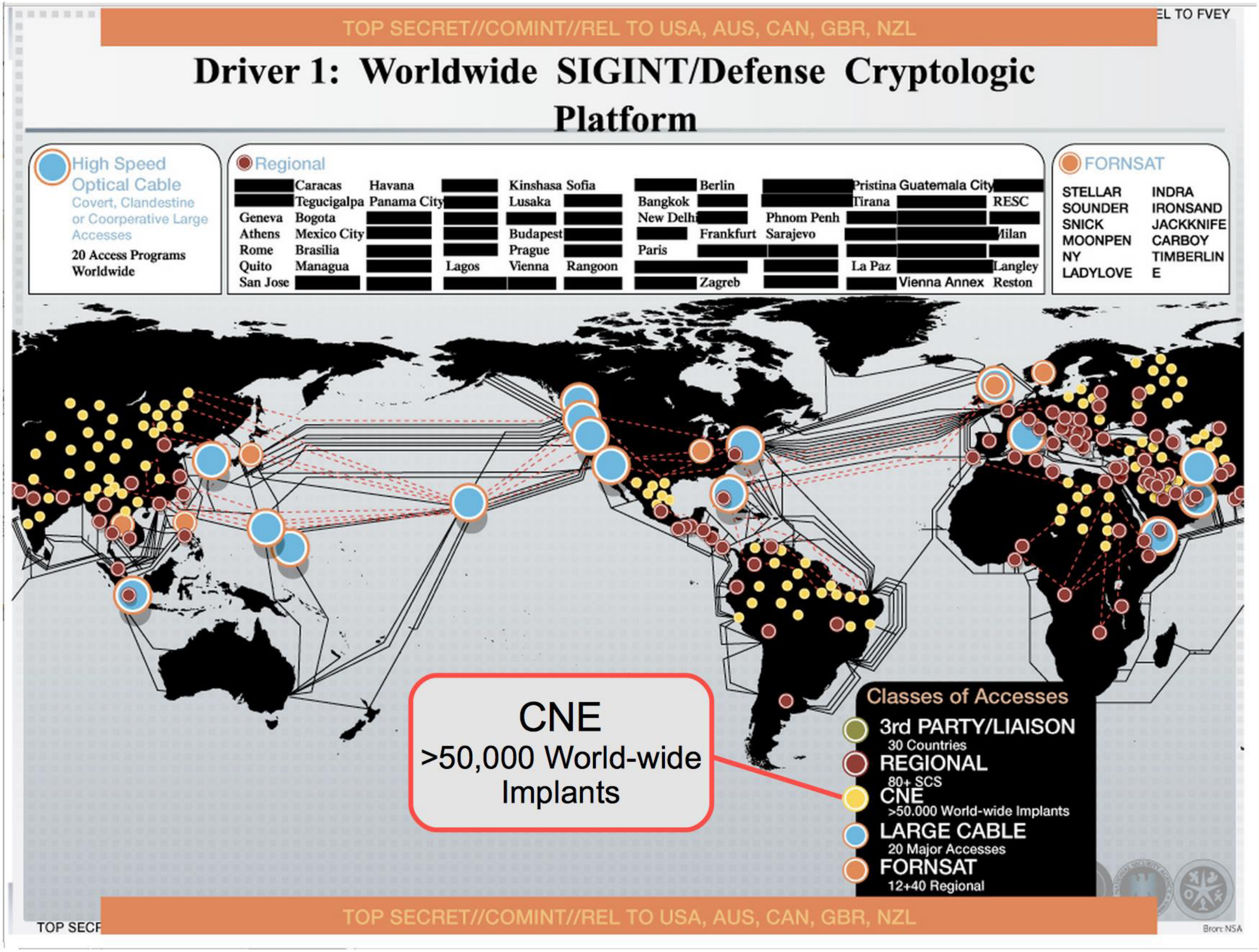
(TS//SI//NF) On 31 July, Microsoft (MS) began encrypting web-based chat with the introduction of the new outlook.com service. This new Secure Socket Layer (SSL) encryption effectively cut off collection of the new service for FAA 702 and likely 12333 (to some degree) for the Intelligence Community (IC). MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012. The SSL solution was applied to all current FISA and 702/PRISM requirements – no changes to UTT tasking procedures were required. The SSL solution does not collect server-based voice/video or file transfers. The MS legacy collection system will remain in place to collect voice/video and file transfers. As a result there will be some duplicate collection of text-based chat from the new and legacy systems which will be addressed at a later date. An increase in collection volume as a result of this solution has already been noted by CES.



(TS//SI//NF) Expanding PRISM Sharing With FBI and CIA

By NAME REDACTED on 2012-08-31 0947

(TS//SI//NF) Special Source Operations (SSO) has recently expanded sharing with the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA) on PRISM operations via two projects. Through these efforts, SSO has created an environment of sharing and teaming across the Intelligence Community on PRISM operations. First, SSO's PRINTAURA team solved a problem for the Signals Intelligence Directorate (SID) by writing software which would automatically gather a list of tasked PRISM selectors every two weeks to provide to the FBI and CIA. This enables our partners to see which selectors the National Security Agency (NSA) has tasked to PRISM. The FBI and CIA then can request a copy of PRISM collection from any selector, as allowed under the 2008 Foreign Intelligence Surveillance Act (FISA) Amendments Act law. Prior to PRINTAURA's work, SID had been providing the FBI and CIA with incomplete and inaccurate lists, preventing our partners from making full use of the PRISM program. PRINTAURA volunteered to gather the detailed data related to each selector from multiple locations and assemble it in a usable form. In the second project, the PRISM Mission Program Manager (MPM) recently began sending operational PRISM news and guidance to the FBI and CIA so that their analysts could task the PRISM system properly, be aware of outages and changes, and optimize their use of PRISM. The MPM coordinated an agreement from the SID Foreign Intelligence Surveillance Act Amendments Act (FAA) Team to share this information weekly, which has been well-received and appreciated. These two activities underscore the point that PRISM is a team sport!



EL TO FVEY

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses
20 Access Programs Worldwide

Regional

[redacted] Caracas Havana [redacted] Kinshasa Sofia [redacted] Berlin [redacted] Pristina Guatemala City [redacted]
[redacted] Tegucigalpa Panama City [redacted] Lusaka [redacted] Bangkok [redacted] [redacted] Tirana [redacted] RESC
Geneva Bogota [redacted] [redacted] [redacted] [redacted] New Delhi [redacted] Phnom Penh [redacted] [redacted] [redacted]
Athens Mexico City [redacted] [redacted] Budapest [redacted] [redacted] Frankfurt Sarajevo [redacted] [redacted]ilan
Rome Brasilia [redacted] [redacted] Prague [redacted] Paris [redacted] [redacted] [redacted] [redacted] [redacted]
Quito Managua [redacted] Lagos Vienna Rangoon [redacted] [redacted] La Paz [redacted] Langley
San Jose [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] Zagreb [redacted] [redacted] Vienna Annex Reston

FORNSAT

STELLAR
SOUNDER
SNICK
MOONPEN
NY
LADYLOVE
INDRA
IRONSAND
JACKKNIFE
CARBOY
TIMBERLIN
E

CNE
>50,000 World-wide Implants

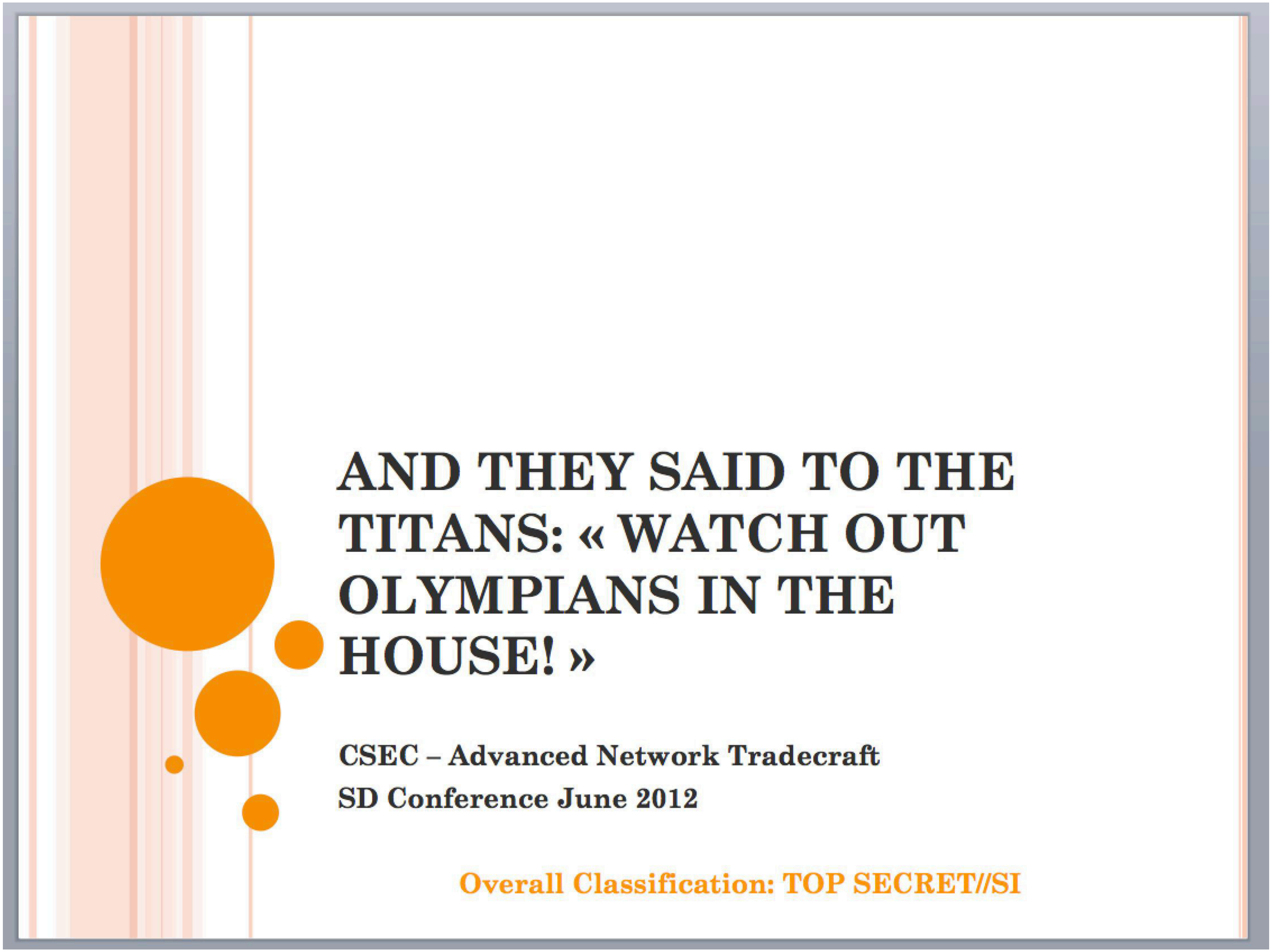
Classes of Accesses

- 3rd PARTY/LIAISON
  30 Countries
- REGIONAL
  80+ SCS
- CNE
  >50.000 World-wide Implants
- LARGE CABLE
  20 Major Accesses
- FORNSAT
  12+40 Regional

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

TOP SECR

Bron: NSA

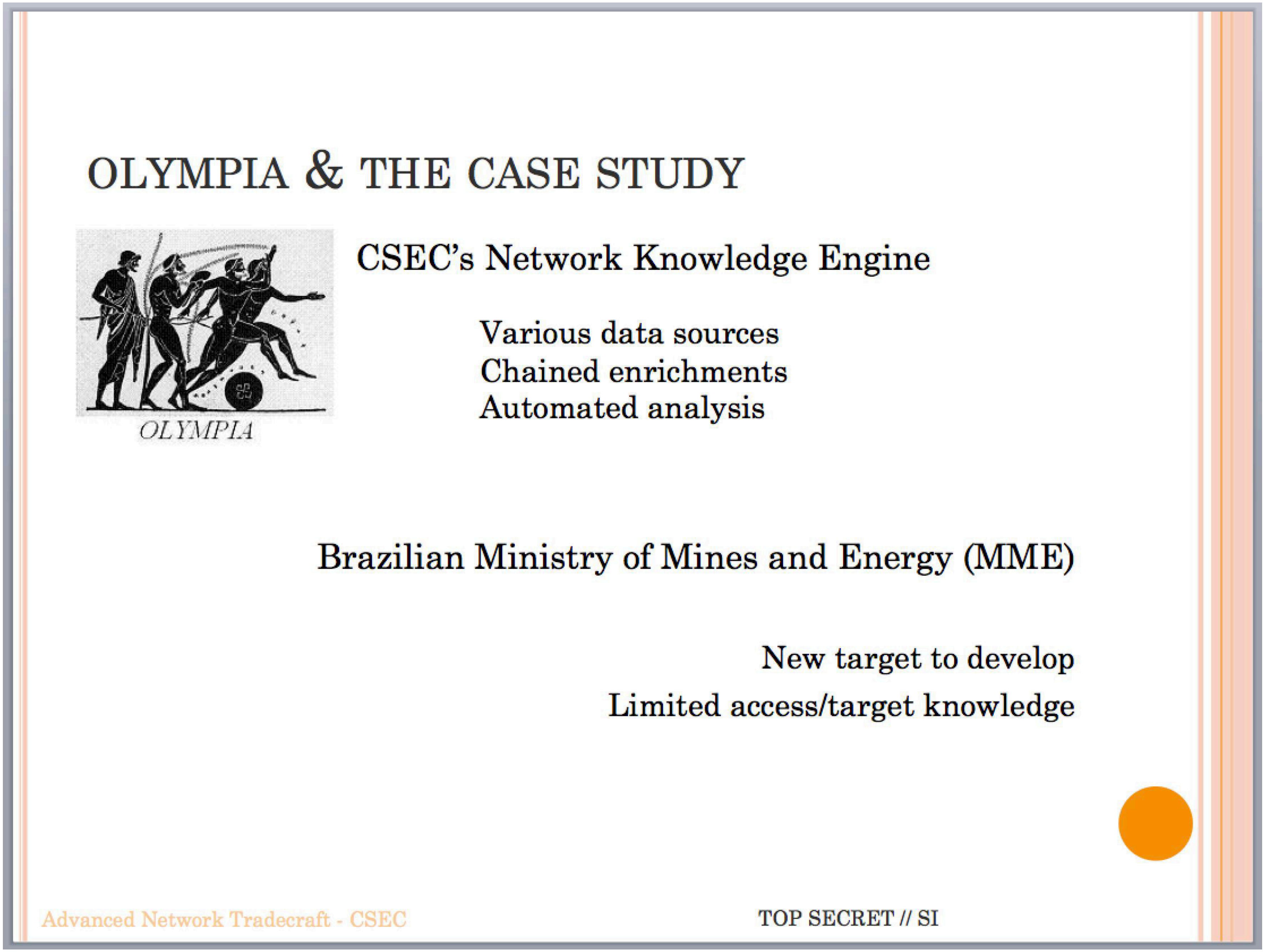


AND THEY SAID TO THE TITANS: « WATCH OUT OLYMPIANS IN THE HOUSE! »

CSEC – Advanced Network Tradecraft

SD Conference June 2012

Overall Classification: TOP SECRET//SI



OLYMPIA & THE CASE STUDY

OLYMPIA

CSEC's Network Knowledge Engine

Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop

Limited access/target knowledge

TOP SECRET//SI//REL USA, FVEY

National Security Agency/
Central Security Service

3 April 2013

Information Paper

Subject: (U//FOUO) NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)

TOP SECRET//SI//REL TO USA, CAN

(U) What NSA provides to the partner:

(S//SI//REL TO USA, CAN) SIGINT: NSA and CSEC cooperate in targeting approximately 20 high-priority countries [redacted] NSA shares technological developments, cryptologic capabilities, software and resources for state-of-the-art collection, processing and analytic efforts, and IA capabilities. The intelligence exchange with CSEC covers worldwide national and transnational targets. No Consolidated Cryptologic Program (CCP) money is allocated to CSEC, but NSA at times pays R&D and technology costs on shared projects with CSEC.

(U) What the partner provides to NSA:

(TS//SI///REL TO USA, CAN) CSEC offers resources for advanced collection, processing and analysis, and has opened covert sites at the request of NSA. CSEC shares with NSA their unique geographic access to areas unavailable to the U.S. [redacted] and provides cryptographic products, cryptanalysis, technology, and software. CSEC has increased its investment in R&D projects of mutual interest.

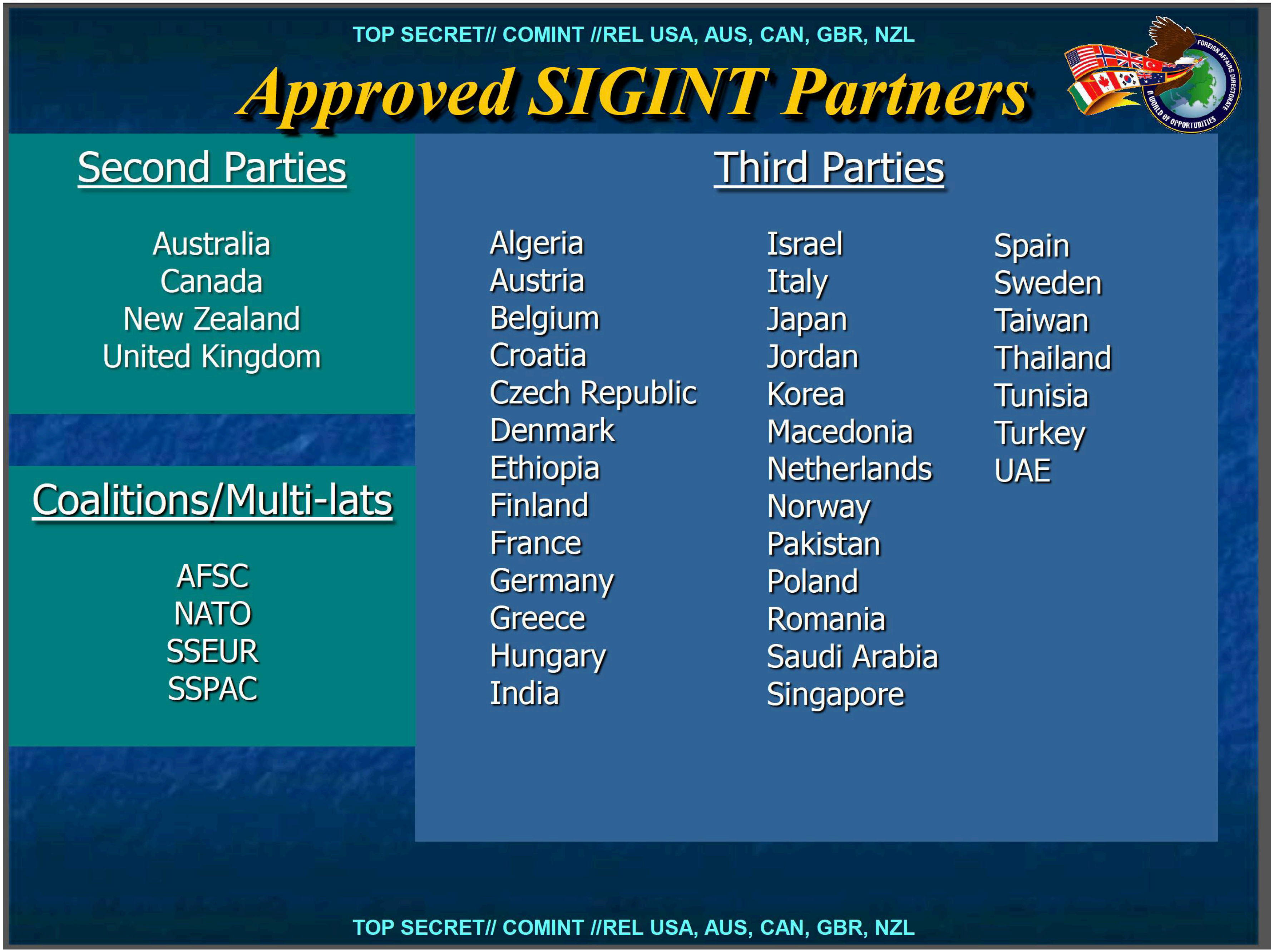
While we have invested significant analytic and collection effort of our own to find and exploit these communications, the difficulties we face in obtaining regular and reliable access to such communications impacts on our ability to detect and prevent terrorist acts and diminishes our capacity to protect the life and safety of Australian citizens and those of our close friends and allies.

We have enjoyed a long and very productive partnership with NSA in obtaining minimised access to United States warranted collection against our highest value terrorist targets in Indonesia. This access has been critical to DSD's efforts to disrupt and contain the operational capabilities of terrorists in our region as highlighted by the recent arrest of fugitive Bali bomber Umar Patek.

We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities – in particular Australians involved with AQAP.

CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary
	Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey


FOREIGN AFFAIRS DIRECTORATE
A WORLD OF OPPORTUNITIES

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

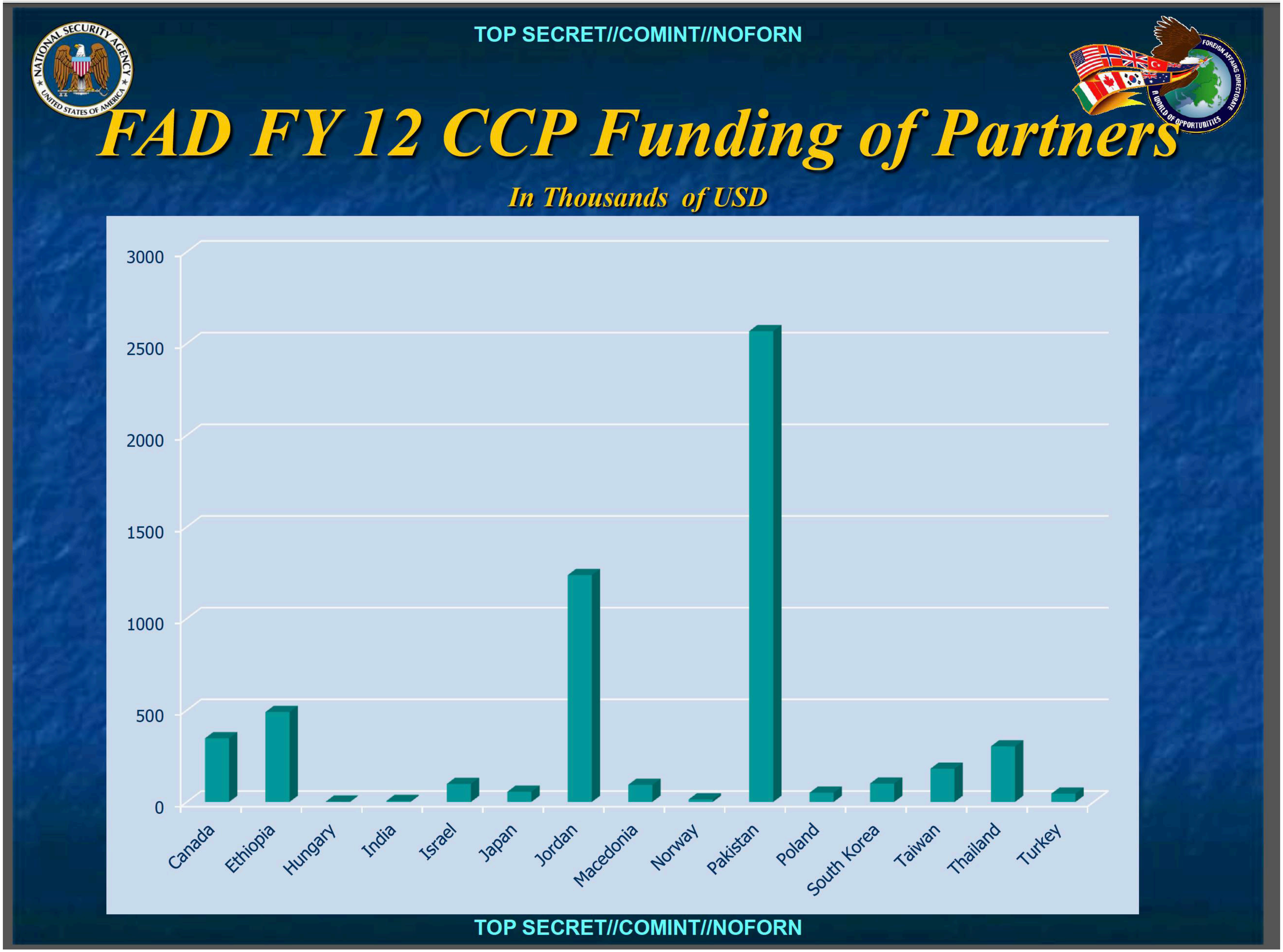
Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//NOFORN

FAD FY 12 CCP Funding of Partners

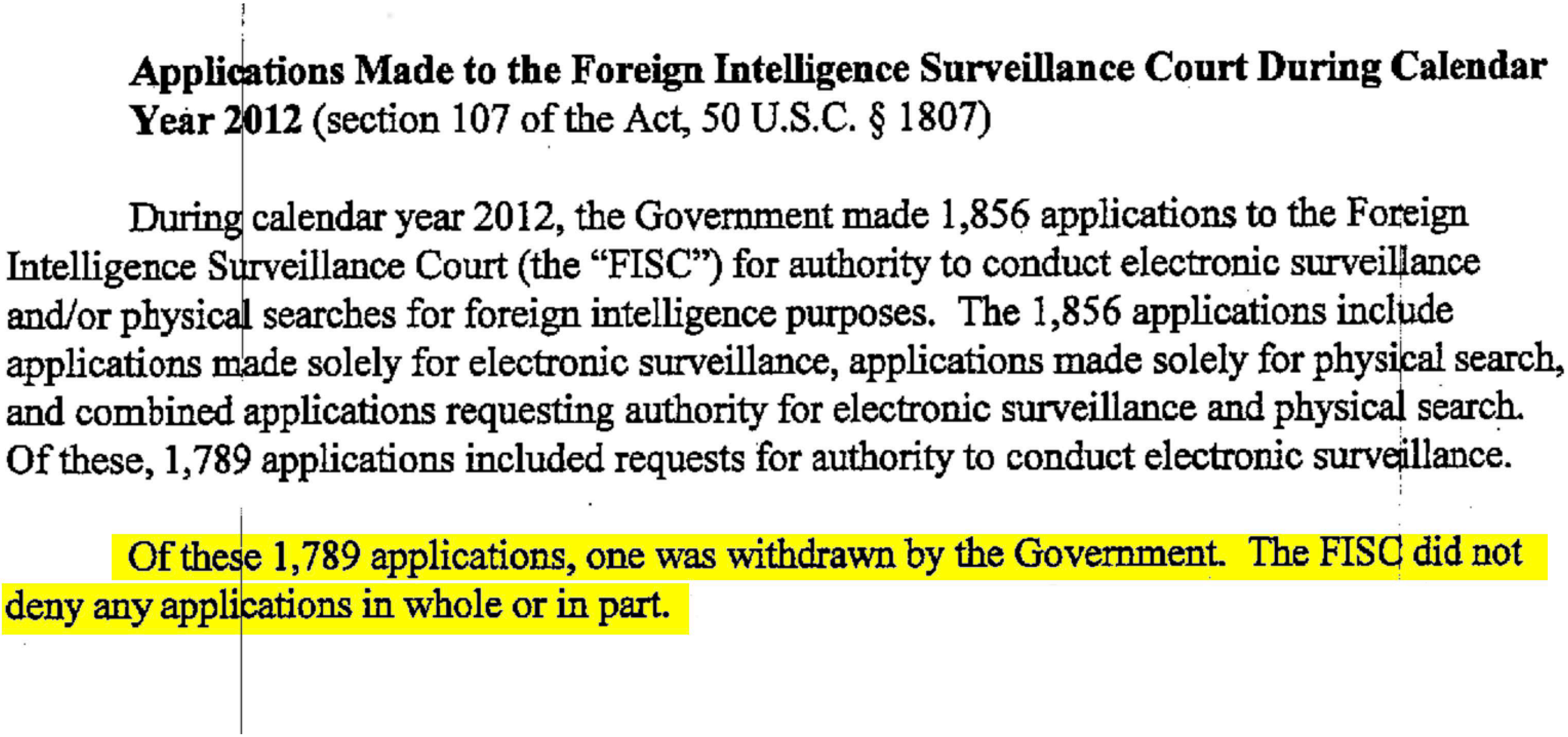
In Thousands of USD

TOP SECRET//COMINT//NOFORN

(TS//SI//REL) There are also a few surprises... France targets the US DoD through technical intelligence collection, and Israel also targets us. On the one hand, the Israelis are extraordinarily good SIGINT partners for us, but on the other, they target us to learn our positions on Middle East problems. A NIE [National Intelligence Estimate] ranked them as the third most aggressive intelligence service against the US.

Page 125

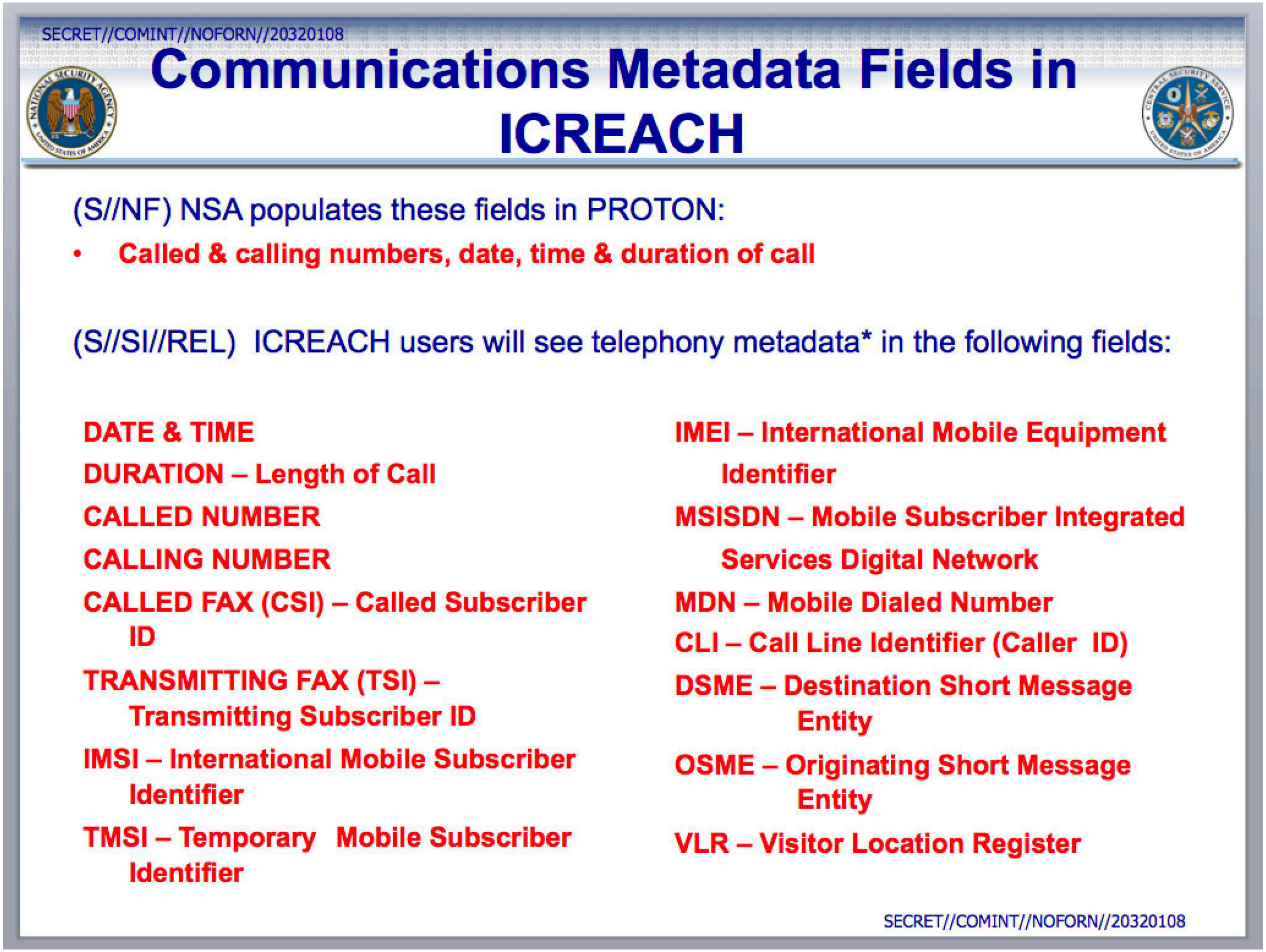
Balancing the SIGINT exchange equally between US and Israeli needs has been a constant challenge in the last decade, it arguably tilted heavily in favor of Israeli security concerns. 9/11 came, and went, with NSA's only true Third Party CT relationship being driven almost totally by the needs of the partner.



Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance.

Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part.



SECRET//COMINT//NOFORN//20320108

Communications Metadata Fields in ICREACH

(S//NF) NSA populates these fields in PROTON:

- Called & calling numbers, date, time & duration of call

(S//SI//REL) ICREACH users will see telephony metadata* in the following fields:

DATE & TIME

DURATION – Length of Call

CALLED NUMBER

CALLING NUMBER

CALLED FAX (CSI) – Called Subscriber ID

TRANSMITTING FAX (TSI) – Transmitting Subscriber ID

IMSI – International Mobile Subscriber Identifier

TMSI – Temporary Mobile Subscriber Identifier

IMEI – International Mobile Equipment Identifier

MSISDN – Mobile Subscriber Integrated Services Digital Network

MDN – Mobile Dialed Number

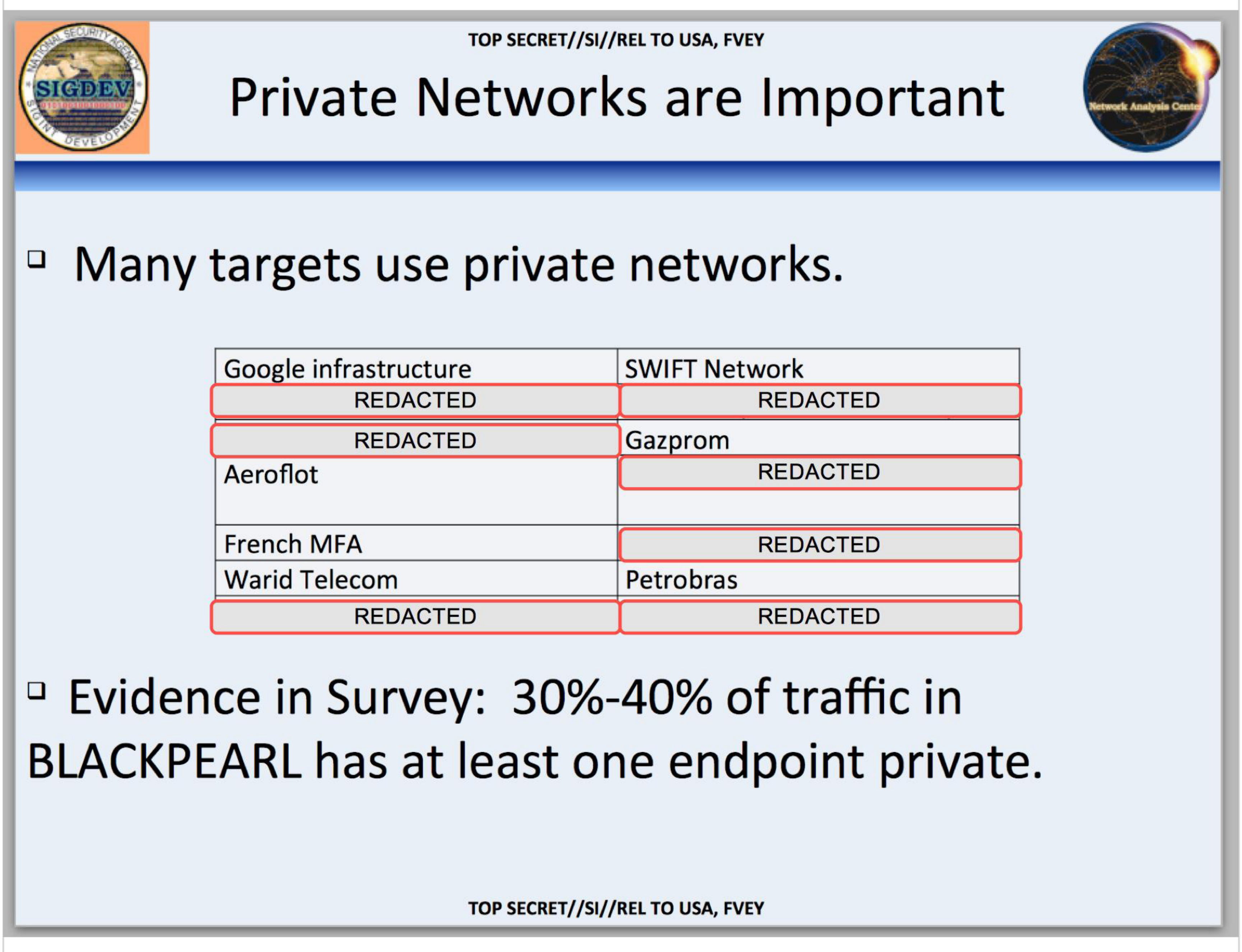
CLI – Call Line Identifier (Caller ID)

DSME – Destination Short Message Entity

OSME – Originating Short Message Entity

VLR – Visitor Location Register

SECRET//COMINT//NOFORN//20320108



TOP SECRET//SI//REL TO USA, FVEY

Private Networks are Important

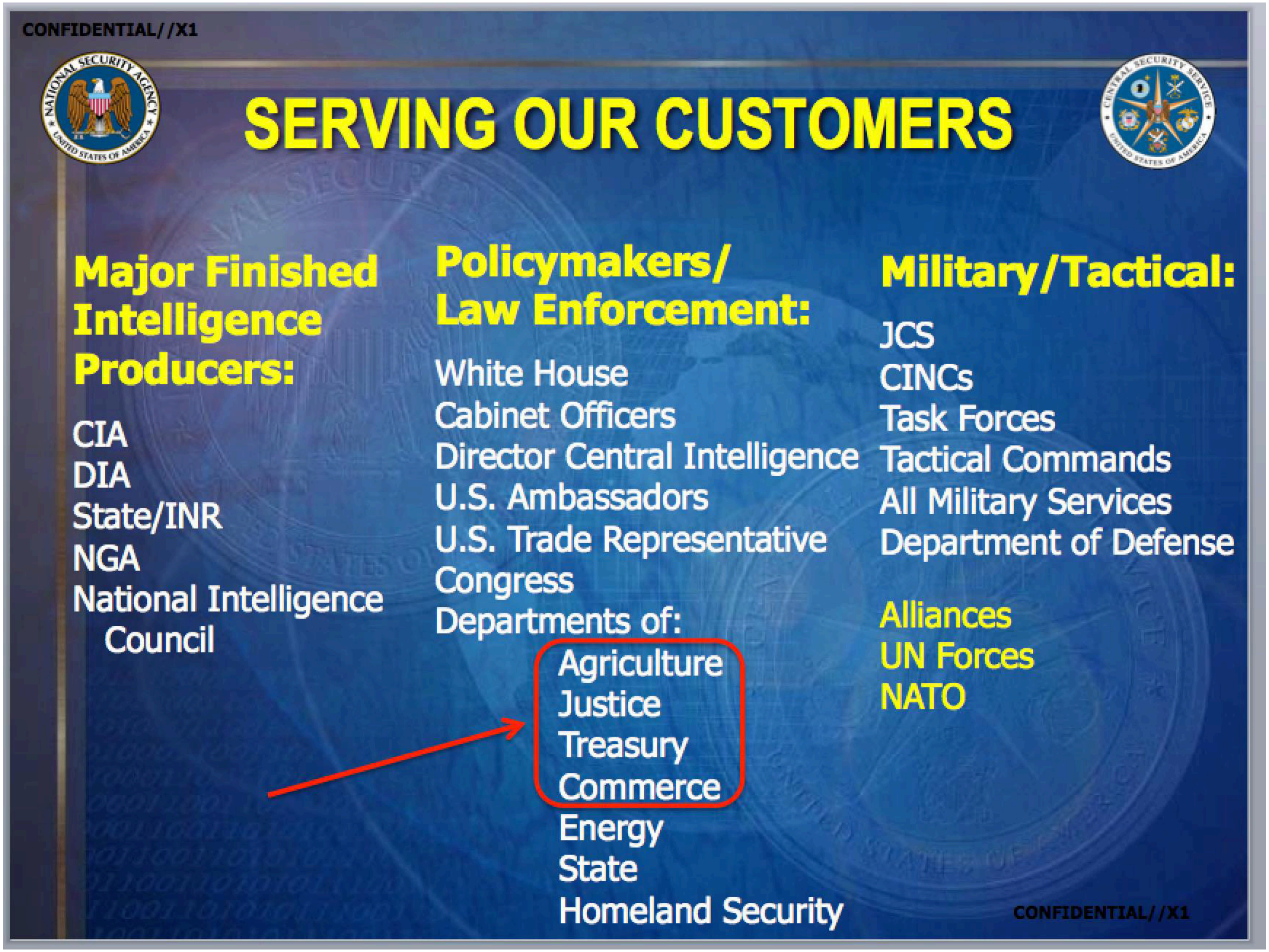
- Many targets use private networks.

Google infrastructure	SWIFT Network
REDACTED	REDACTED
REDACTED	Gazprom
Aeroflot	REDACTED
French MFA	REDACTED
Warid Telecom	Petrobras
REDACTED	REDACTED

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.

TOP SECRET//SI//REL TO USA, FVEY

Page 136



CONFIDENTIAL//X1

SERVING OUR CUSTOMERS

Major Finished Intelligence Producers:

CIA
DIA
State/INR
NGA
National Intelligence
Council

Policymakers/ Law Enforcement:

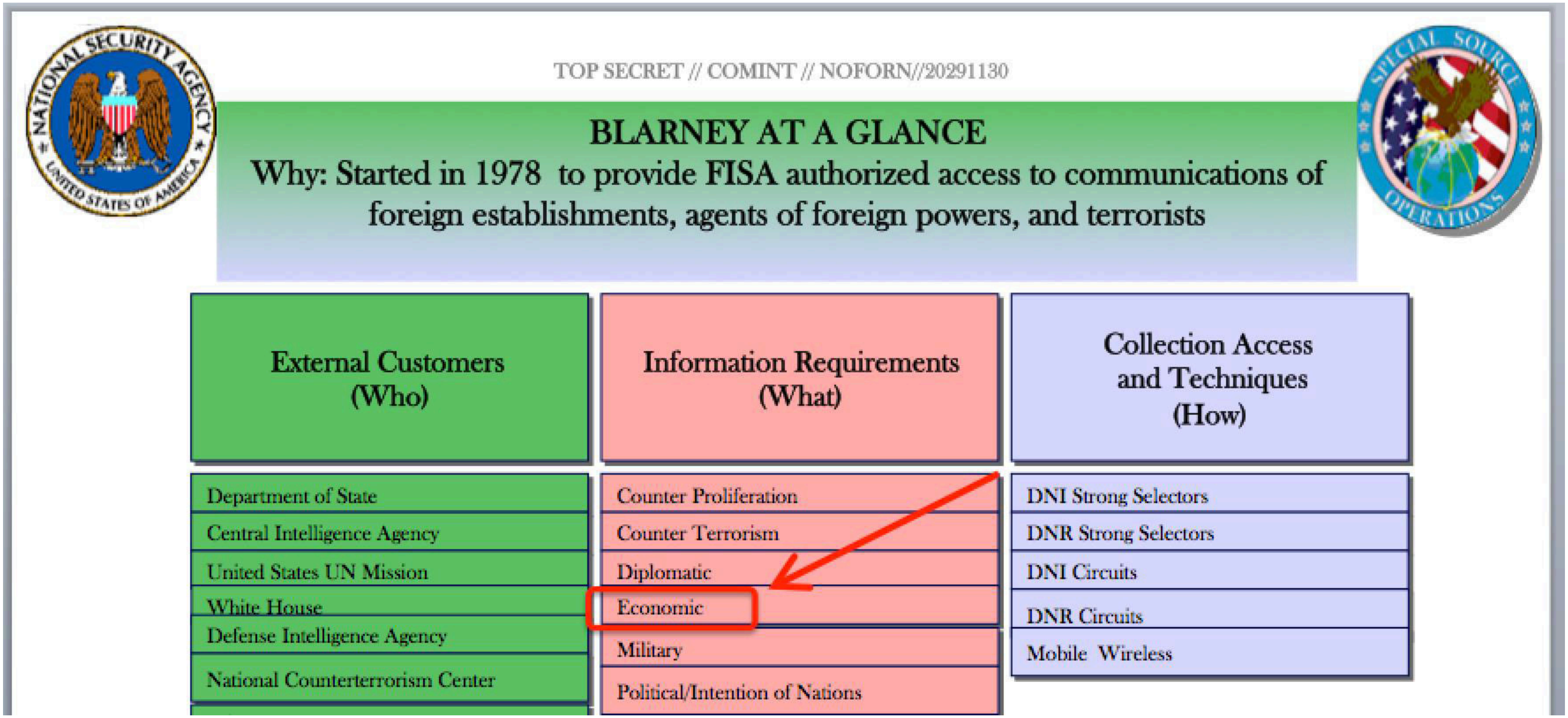
White House
Cabinet Officers
Director Central Intelligence
U.S. Ambassadors
U.S. Trade Representative
Congress
Departments of:
Agriculture
Justice
Treasury
Commerce
Energy
State
Homeland Security

Military/Tactical:

JCS
CINCs
Task Forces
Tactical Commands
All Military Services
Department of Defense

Alliances
UN Forces
NATO

CONFIDENTIAL//X1

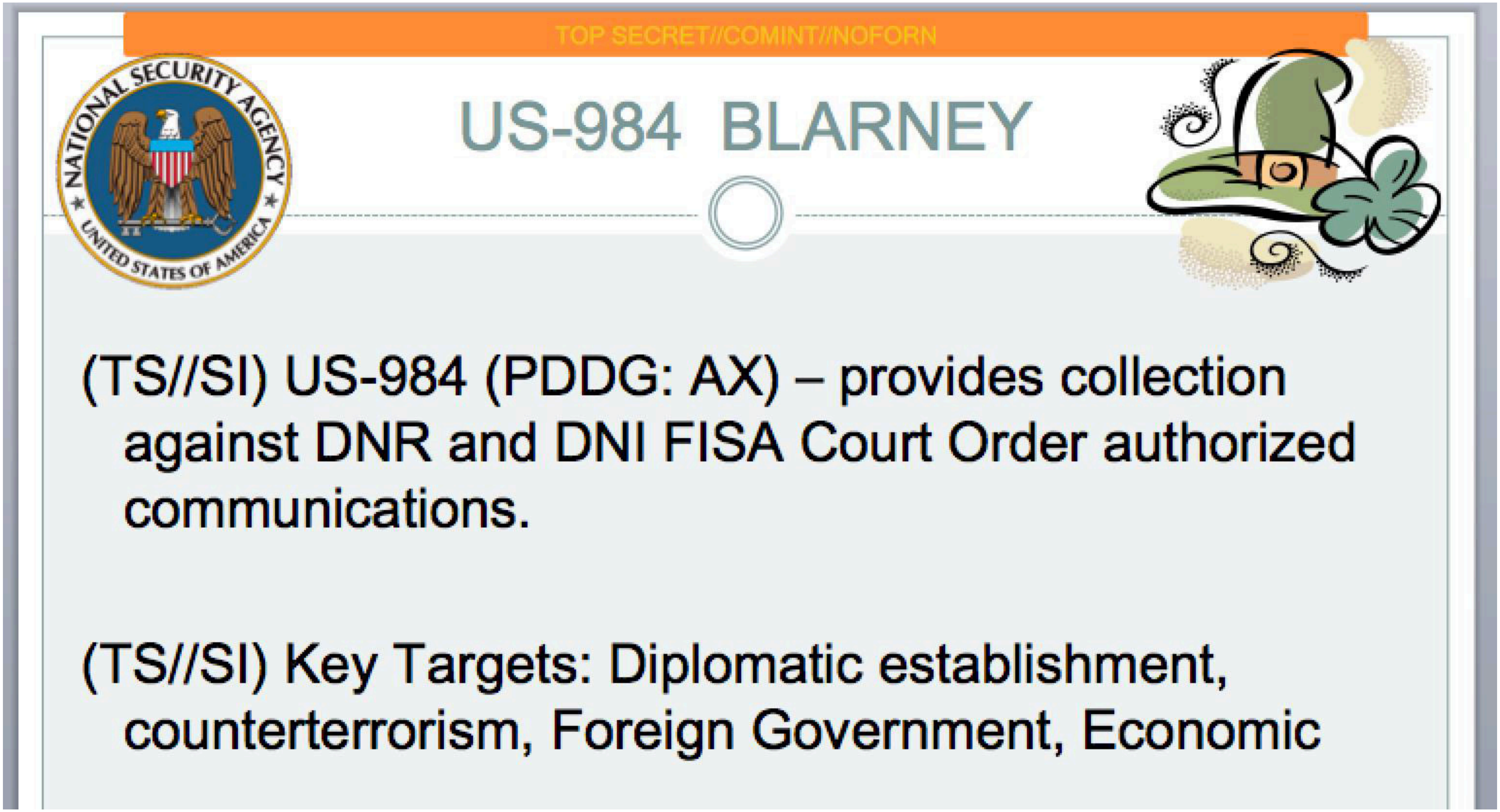


TOP SECRET // COMINT // NOFORN//20291130

BLARNEY AT A GLANCE

Why: Started in 1978 to provide FISA authorized access to communications of foreign establishments, agents of foreign powers, and terrorists

External Customers (Who)	Information Requirements (What)	Collection Access and Techniques (How)
Department of State	Counter Proliferation	DNI Strong Selectors
Central Intelligence Agency	Counter Terrorism	DNR Strong Selectors
United States UN Mission	Diplomatic	DNI Circuits
White House	Economic	DNR Circuits
Defense Intelligence Agency	Military	Mobile Wireless
National Counterterrorism Center	Political/Intention of Nations	



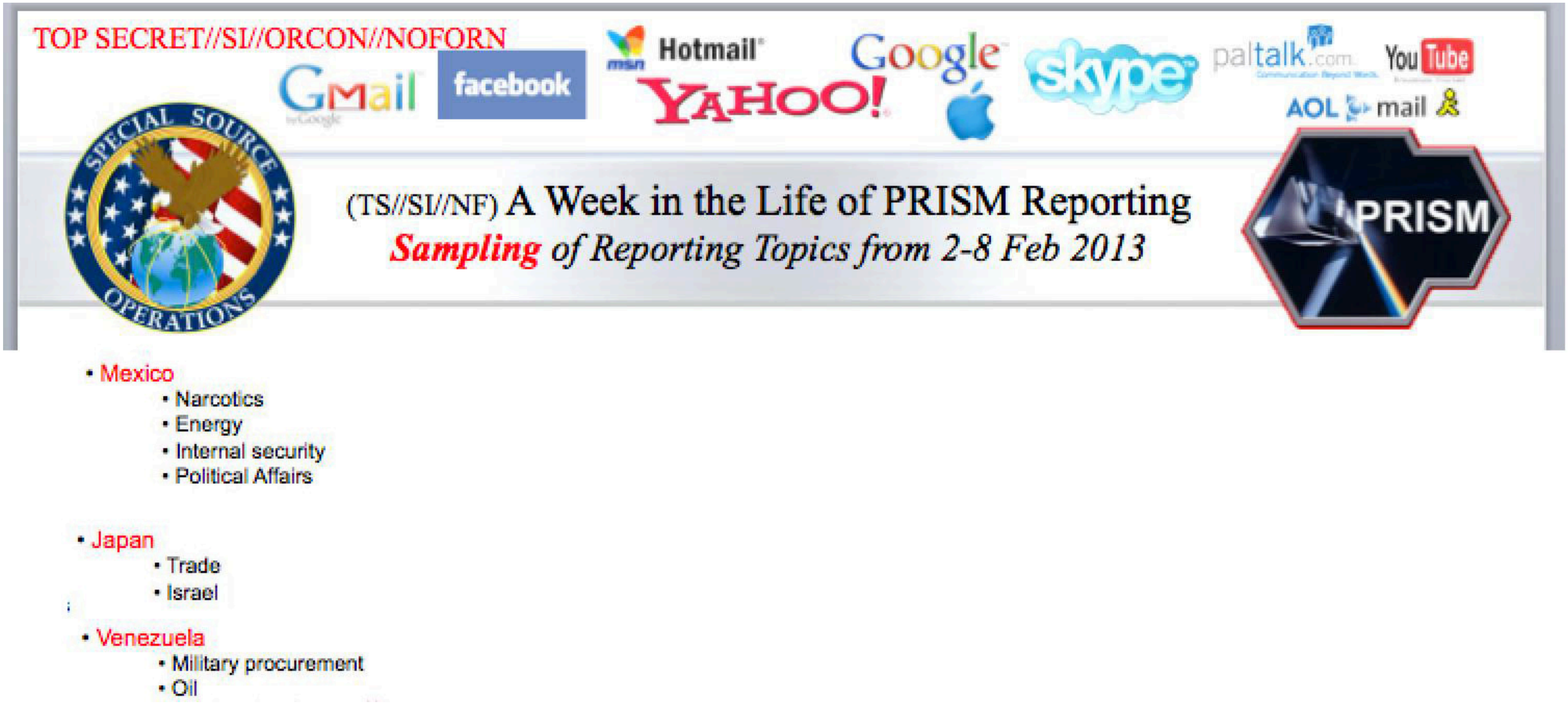
TOP SECRET//COMINT//NOFORN

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

US-984 BLARNEY

(TS//SI) US-984 (PDDG: AX) – provides collection against DNR and DNI FISA Court Order authorized communications.

(TS//SI) Key Targets: Diplomatic establishment, counterterrorism, Foreign Government, Economic


Gmail by Google
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk.com Communication Beyond Words
YouTube Broadcast Yourself
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) A Week in the Life of PRISM Reporting

Sampling of Reporting Topics from 2-8 Feb 2013

- Mexico
  - Narcotics
  - Energy
  - Internal security
  - Political Affairs

- Japan
  - Trade
  - Israel

- Venezuela
  - Military procurement
  - Oil

(U) NSA Washington Mission

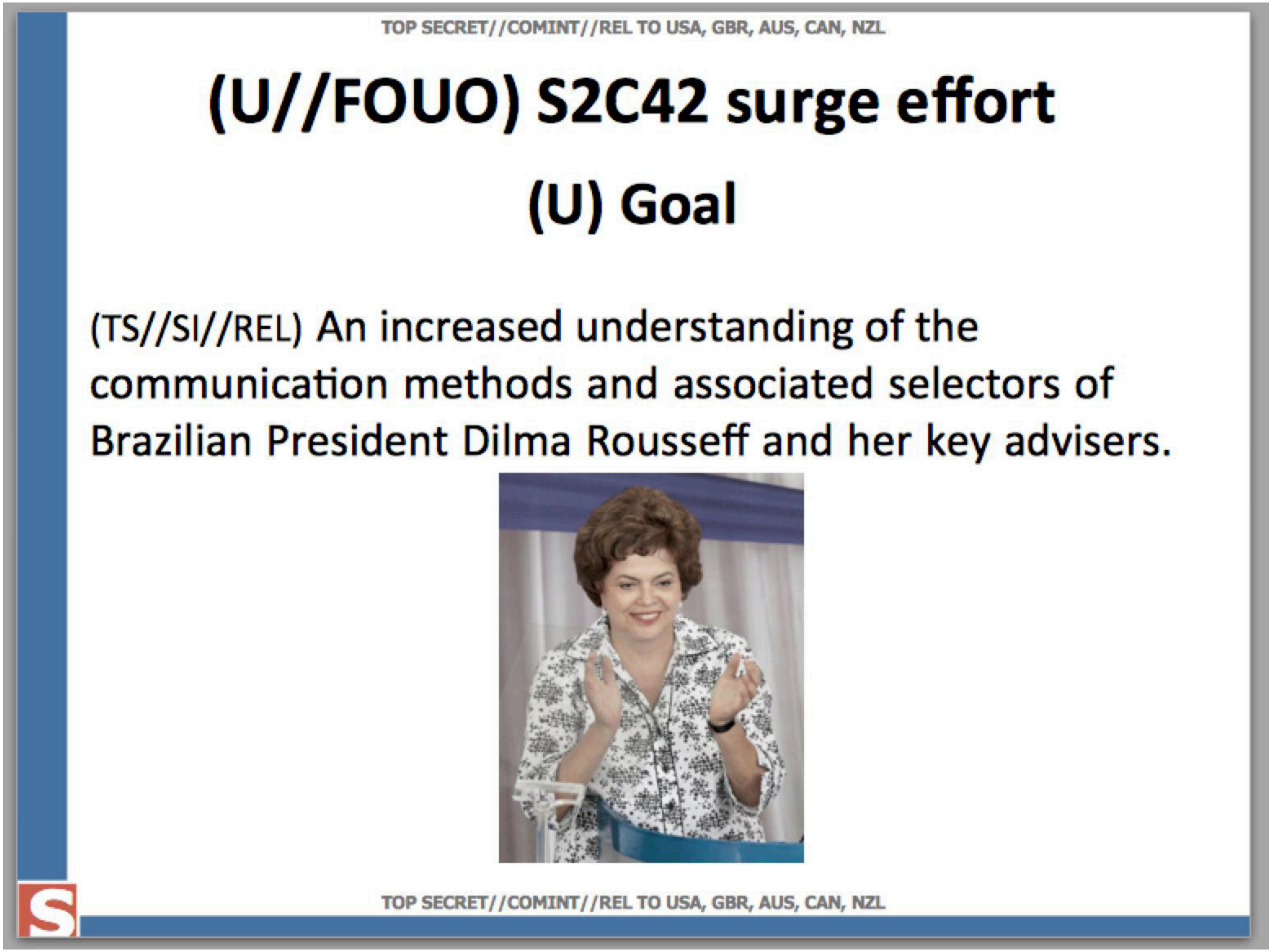
(U) Regional

(TS//SI) ISI is responsible for 13 individual nation states in three continents. One significant tie that binds all these countries together is their importance to U.S. economic, trade, and defense concerns. The Western Europe and Strategic Partnerships division primarily focuses on foreign policy and trade activities of Belgium, France, Germany, Italy, and Spain, as well as Brazil, Japan and Mexico.

(TS//SI) The Energy and Resource branch provides unique intelligence on worldwide energy production and development in key countries that affect the world economy. Targets of current emphasis are [redacted] and the [redacted]. Reporting has included the monitoring of international investment in the energy sectors of target countries, electrical and Supervisory Control and Data Acquisition (SCADA) upgrades, and computer aided designs of projected energy projects.

Page 139

The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues, such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez.



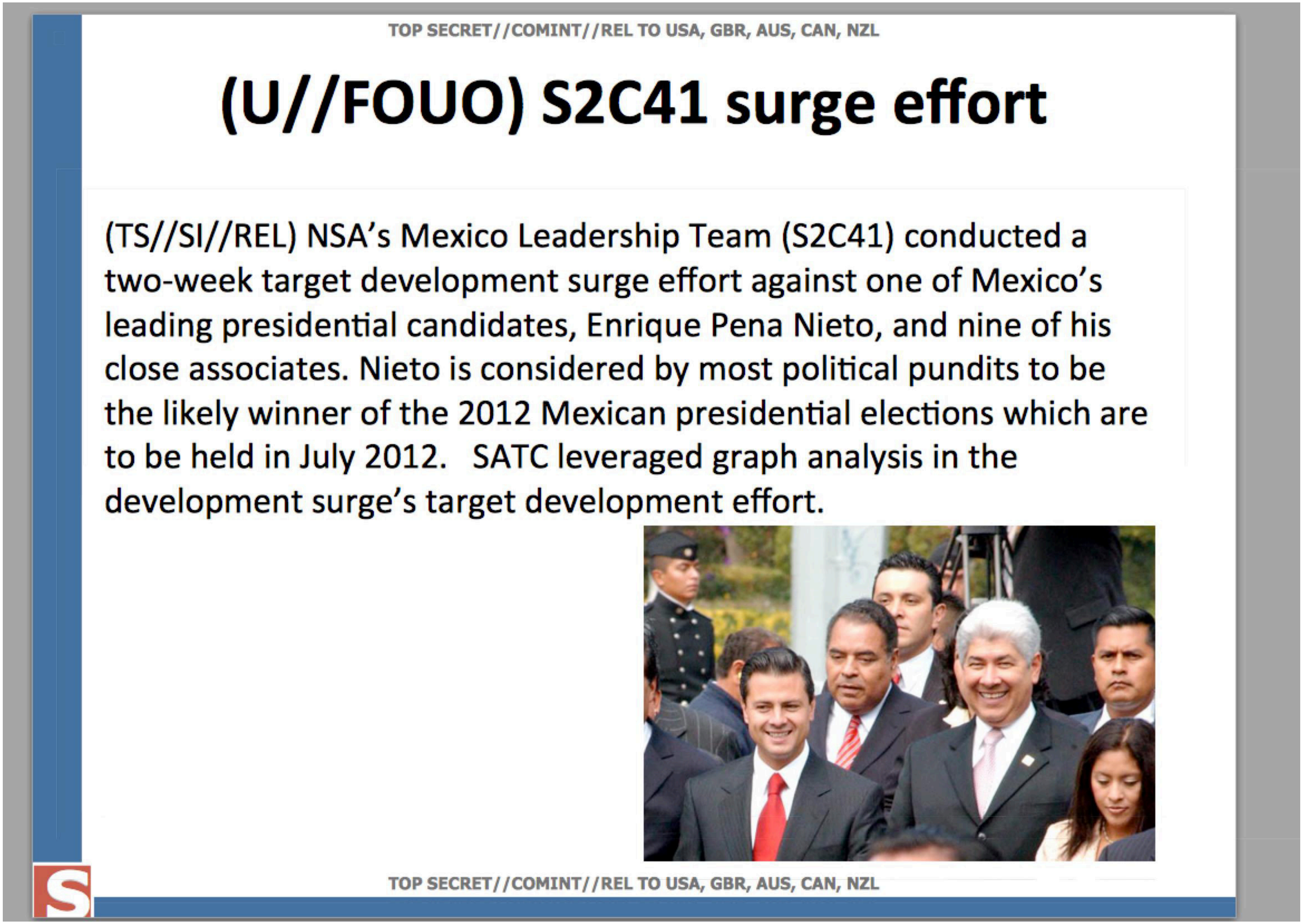
TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

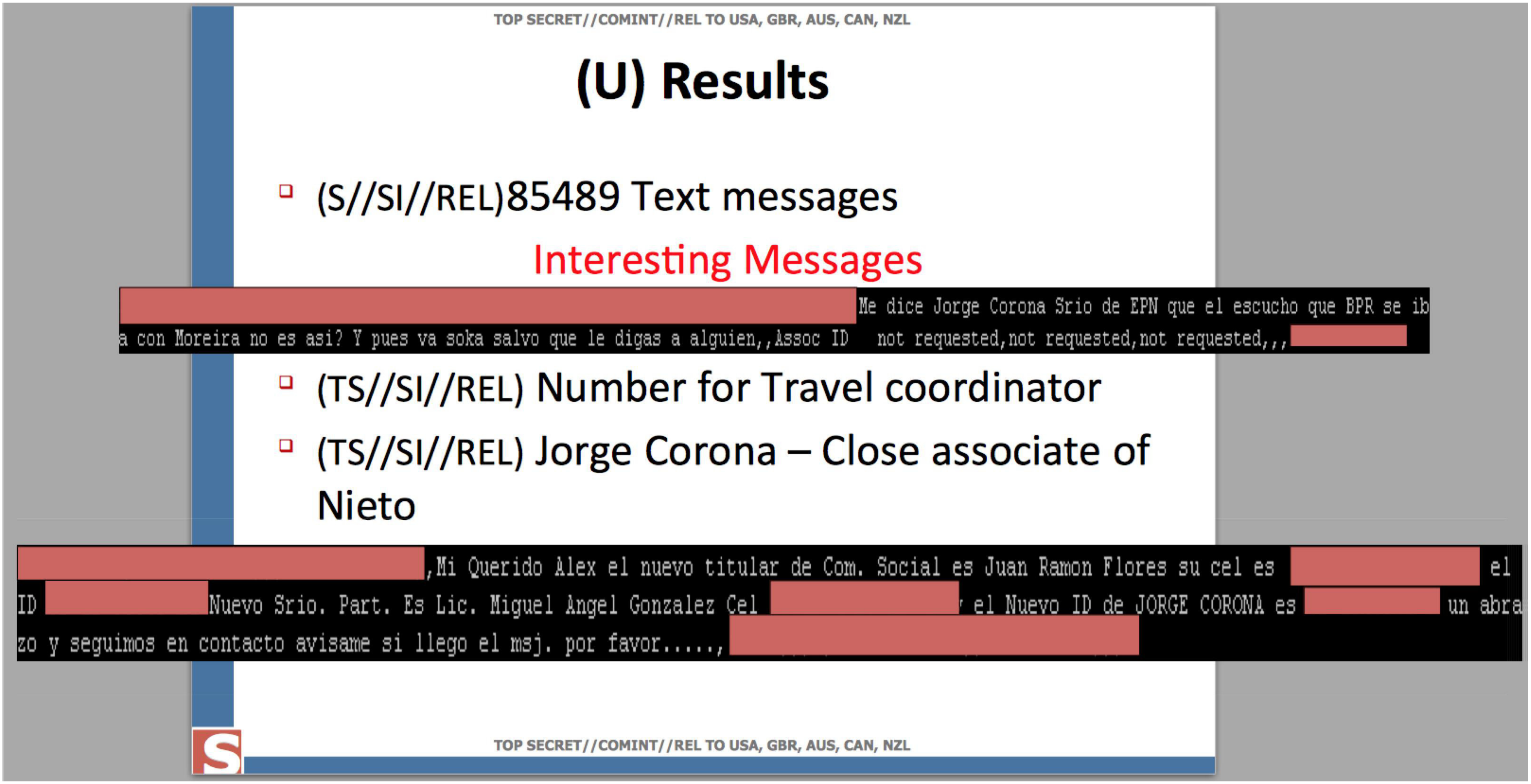
(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL



(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U) Results

- (S//SI//REL)85489 Text messages

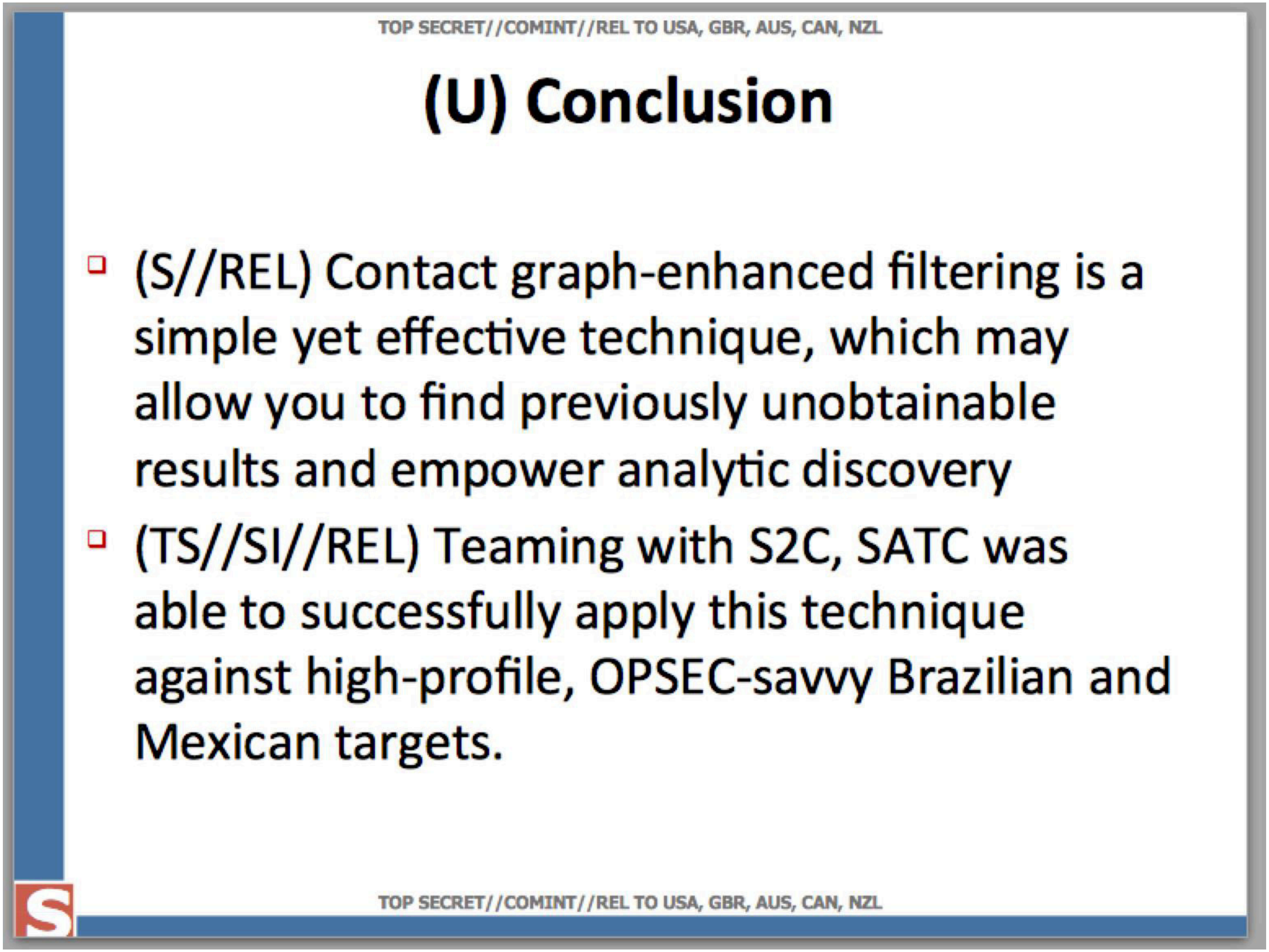
Interesting Messages

[redacted] Me dice Jorge Corona Srio de EPN que el escucho que BPR se iba con Moreira no es asi? Y pues va soka salvo que le digas a alguien,,Assoc ID   not requested,not requested,not requested,,, [redacted]

- (TS//SI//REL) Number for Travel coordinator
- (TS//SI//REL) Jorge Corona – Close associate of Nieto

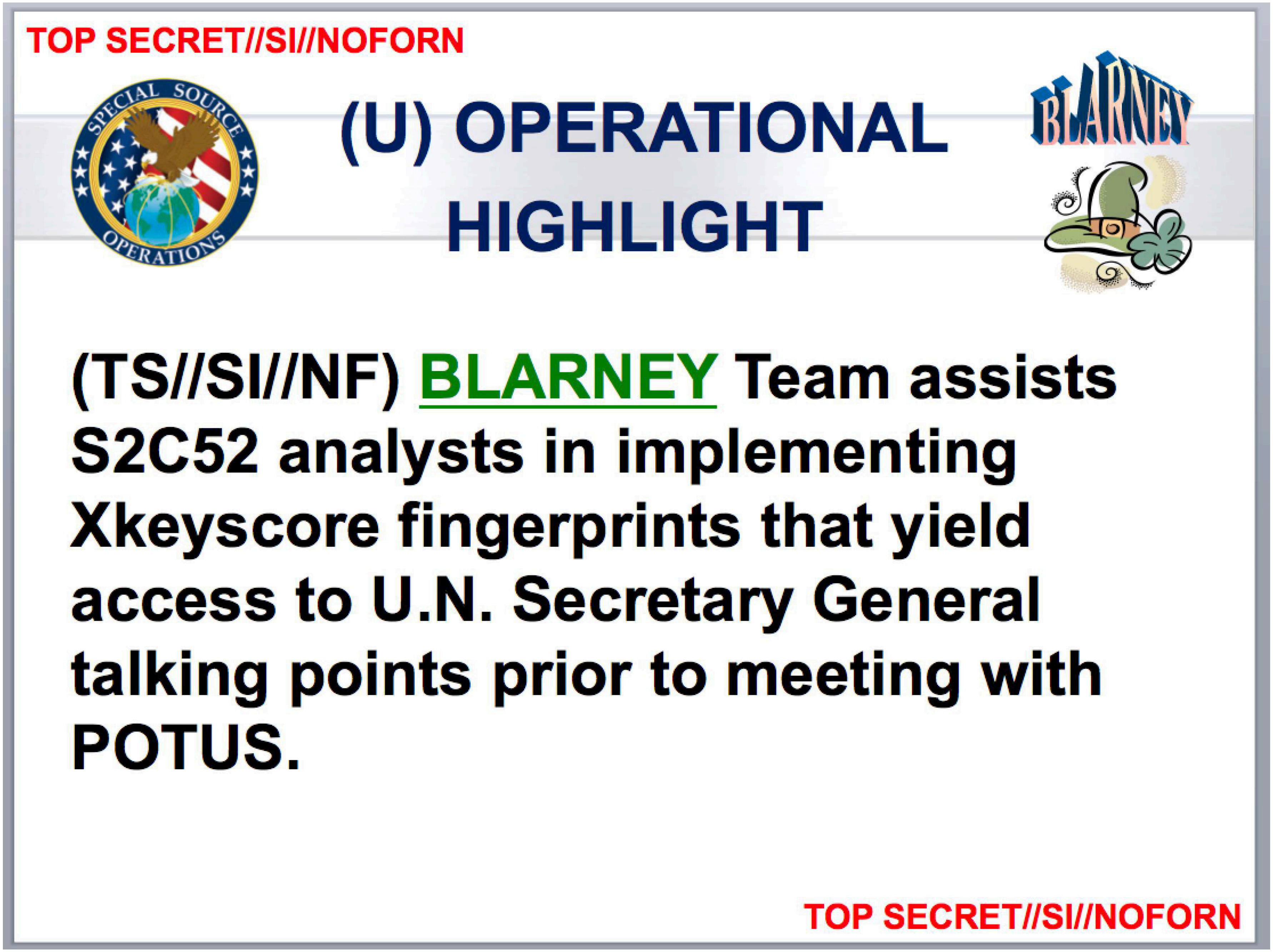
[redacted] ,Mi Querido Alex el nuevo titular de Com. Social es Juan Ramon Flores su cel es [redacted] el ID [redacted] Nuevo Srio. Part. Es Lic. Miguel Angel Gonzalez Cel [redacted] el Nuevo ID de JORGE CORONA es [redacted] un abrazo y seguimos en contacto avisame si llego el msj. por favor....., [redacted]

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL



(U) Conclusion

- (S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery
- (TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.


SPECIAL SOURCE OPERATIONS
BLARNEY

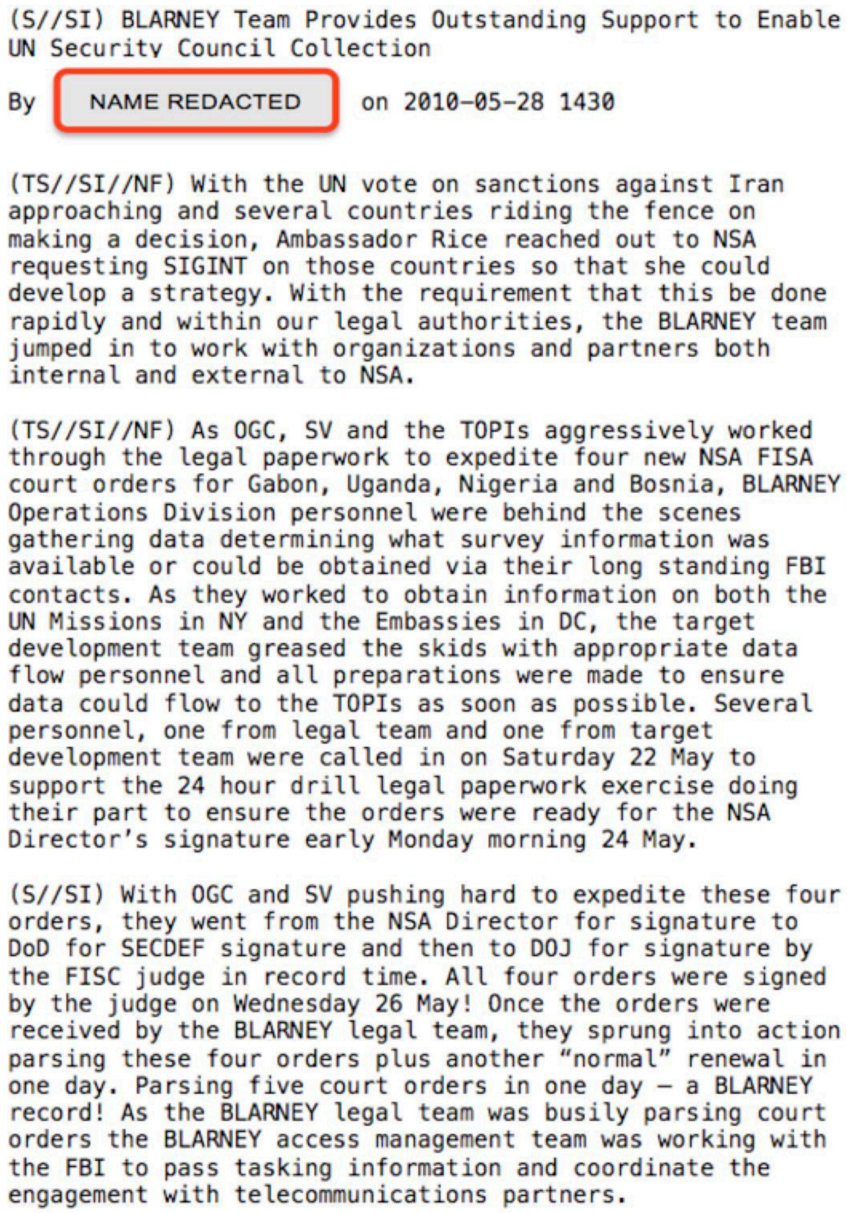
TOP SECRET//SI//NOFORN

(U) OPERATIONAL HIGHLIGHT

(TS//SI//NF) BLARNEY Team assists S2C52 analysts in implementing Xkeyscore fingerprints that yield access to U.N. Secretary General talking points prior to meeting with POTUS.

TOP SECRET//SI//NOFORN

Page 143



(S//SI) BLARNEY Team Provides Outstanding Support to Enable UN Security Council Collection

By NAME REDACTED on 2010-05-28 1430

(TS//SI//NF) With the UN vote on sanctions against Iran approaching and several countries riding the fence on making a decision, Ambassador Rice reached out to NSA requesting SIGINT on those countries so that she could develop a strategy. With the requirement that this be done rapidly and within our legal authorities, the BLARNEY team jumped in to work with organizations and partners both internal and external to NSA.

(TS//SI//NF) As OGC, SV and the TOPIs aggressively worked through the legal paperwork to expedite four new NSA FISA court orders for Gabon, Uganda, Nigeria and Bosnia, BLARNEY Operations Division personnel were behind the scenes gathering data determining what survey information was available or could be obtained via their long standing FBI contacts. As they worked to obtain information on both the UN Missions in NY and the Embassies in DC, the target development team greased the skids with appropriate data flow personnel and all preparations were made to ensure data could flow to the TOPIs as soon as possible. Several personnel, one from legal team and one from target development team were called in on Saturday 22 May to support the 24 hour drill legal paperwork exercise doing their part to ensure the orders were ready for the NSA Director's signature early Monday morning 24 May.

(S//SI) With OGC and SV pushing hard to expedite these four orders, they went from the NSA Director for signature to DoD for SECDEF signature and then to DOJ for signature by the FISC judge in record time. All four orders were signed by the judge on Wednesday 26 May! Once the orders were received by the BLARNEY legal team, they sprung into action parsing these four orders plus another "normal" renewal in one day. Parsing five court orders in one day – a BLARNEY record! As the BLARNEY legal team was busily parsing court orders the BLARNEY access management team was working with the FBI to pass tasking information and coordinate the engagement with telecommunications partners.

TOP SECRET//COMINT//NOFORN

August 2010

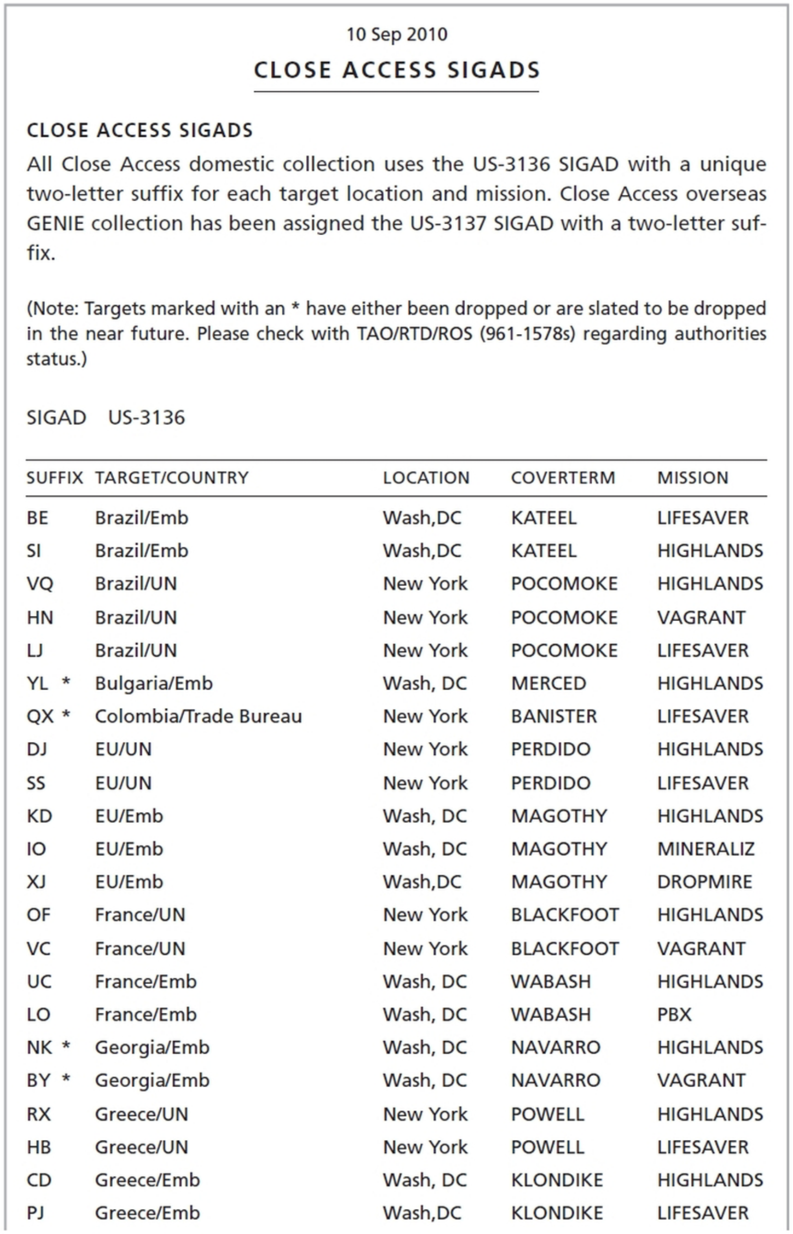
(U//FOUO) Silent Success: SIGINT Synergy Helps Shape US Foreign Policy

(TS//SI//NF) At the outset of these lengthy negotiations, NSA had sustained collection against France Japan, Mexico, Brazil

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) The resolution was adopted by twelve votes for, two against (Brazil and Turkey), and one abstention from Lebanon. According to USUN, SIGINT "helped me to know when the other Permreps [Permanent Representatives] were telling the truth.... revealed their real position on sanctions... gave us an upper hand in negotiations... and provided information on various countries 'red lines.'"

Page 145



10 Sep 2010

CLOSE ACCESS SIGADS

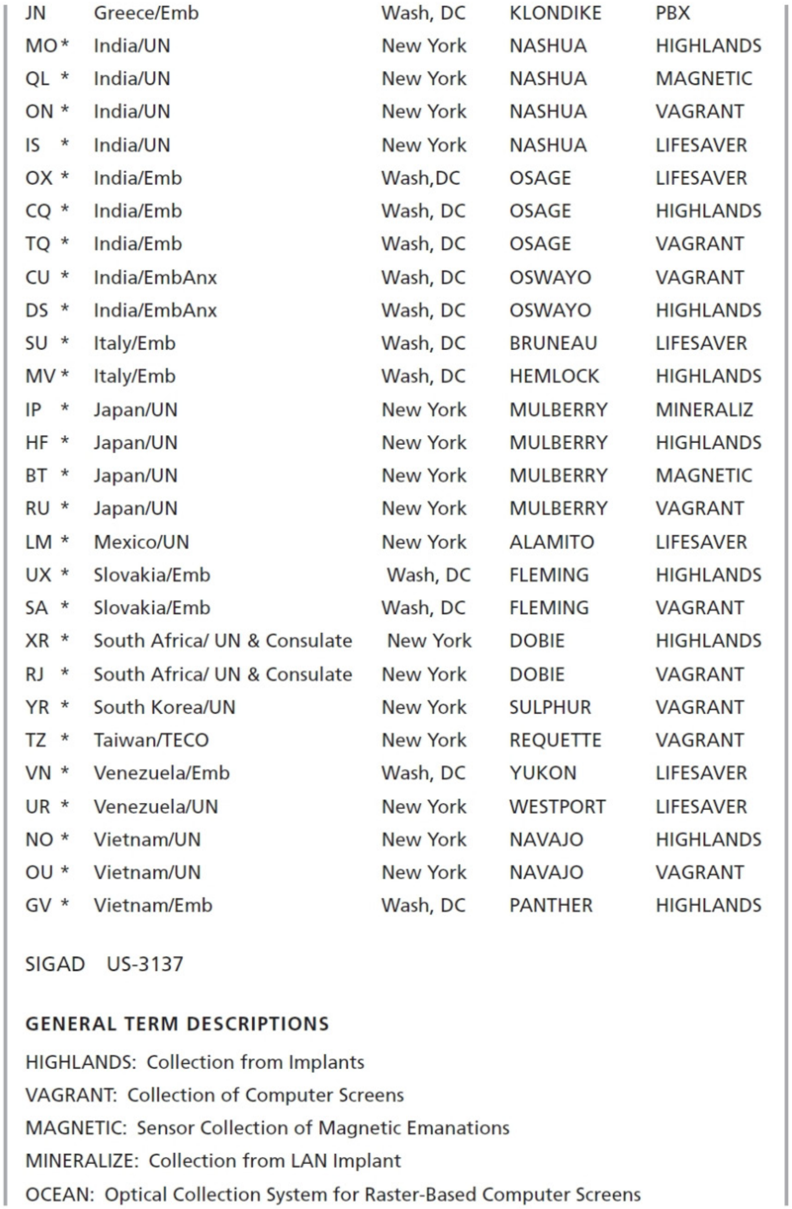
CLOSE ACCESS SIGADS

All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.

(Note: Targets marked with an * have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS (961-1578s) regarding authorities status.)

SIGAD US-3136

SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER



JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO *	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash,DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT
CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS

SIGAD US-3137

GENERAL TERM DESCRIPTIONS

HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Emanations

MINERALIZE: Collection from LAN Implant

OCEAN: Optical Collection System for Raster-Based Computer Screens

LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation; jumping the airgap etc.

BLACKHEART: Collection from an FBI Implant

PBX: Public Branch Exchange Switch

CRYPTO ENABLED: Collection derived from AO's efforts to enable crypto

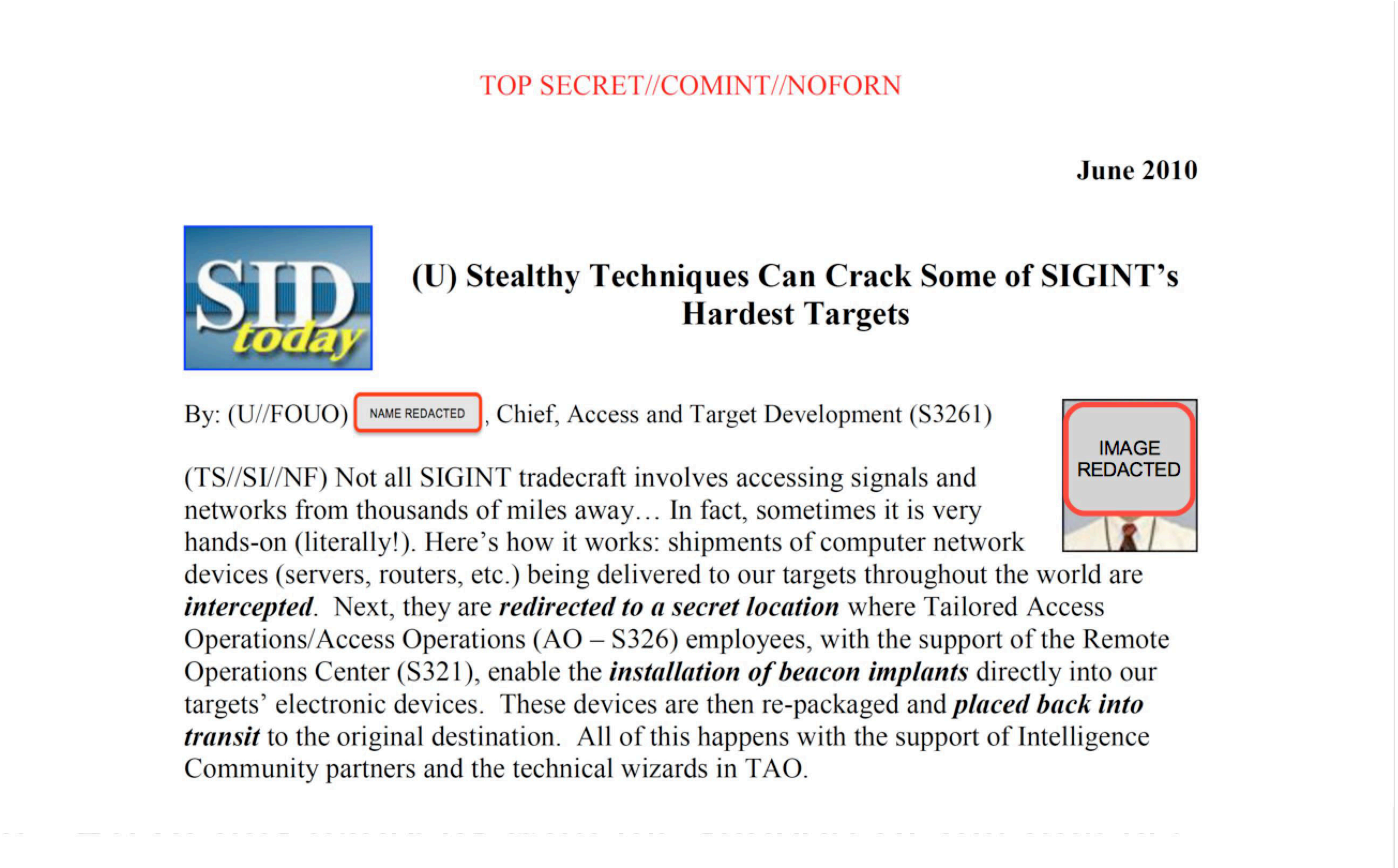
DROPMIRE: passive collection of emanations using an antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access (**NOT** implanted)

DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that provides COVERT link over USB link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.

RADON: Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of Denied networks using standard on-net tools.



TOP SECRET//COMINT//NOFORN

June 2010

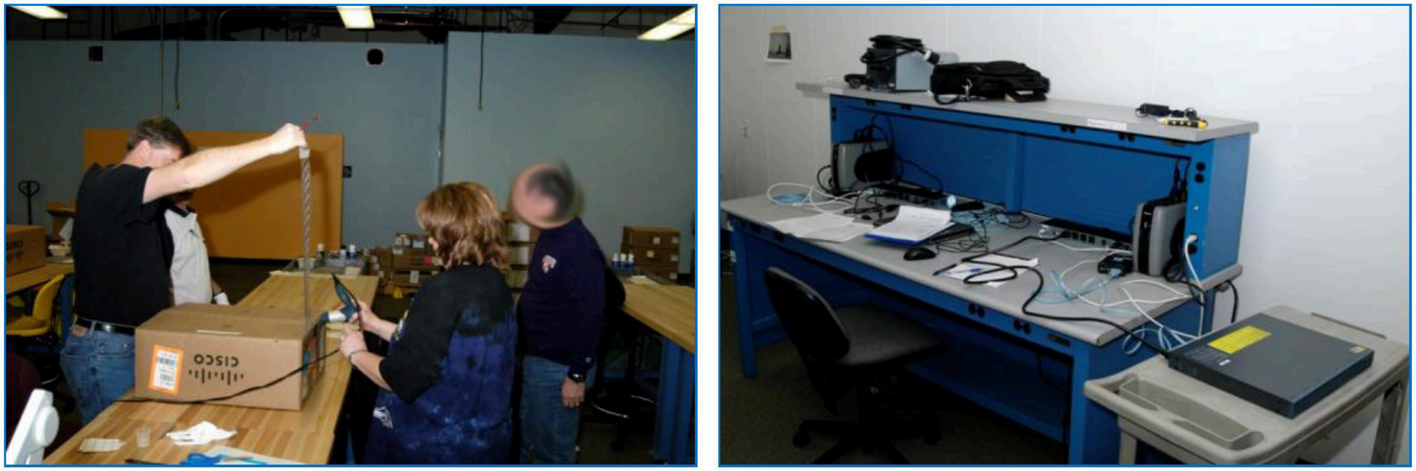
(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) NAME REDACTED, Chief, Access and Target Development (S3261)

IMAGE REDACTED

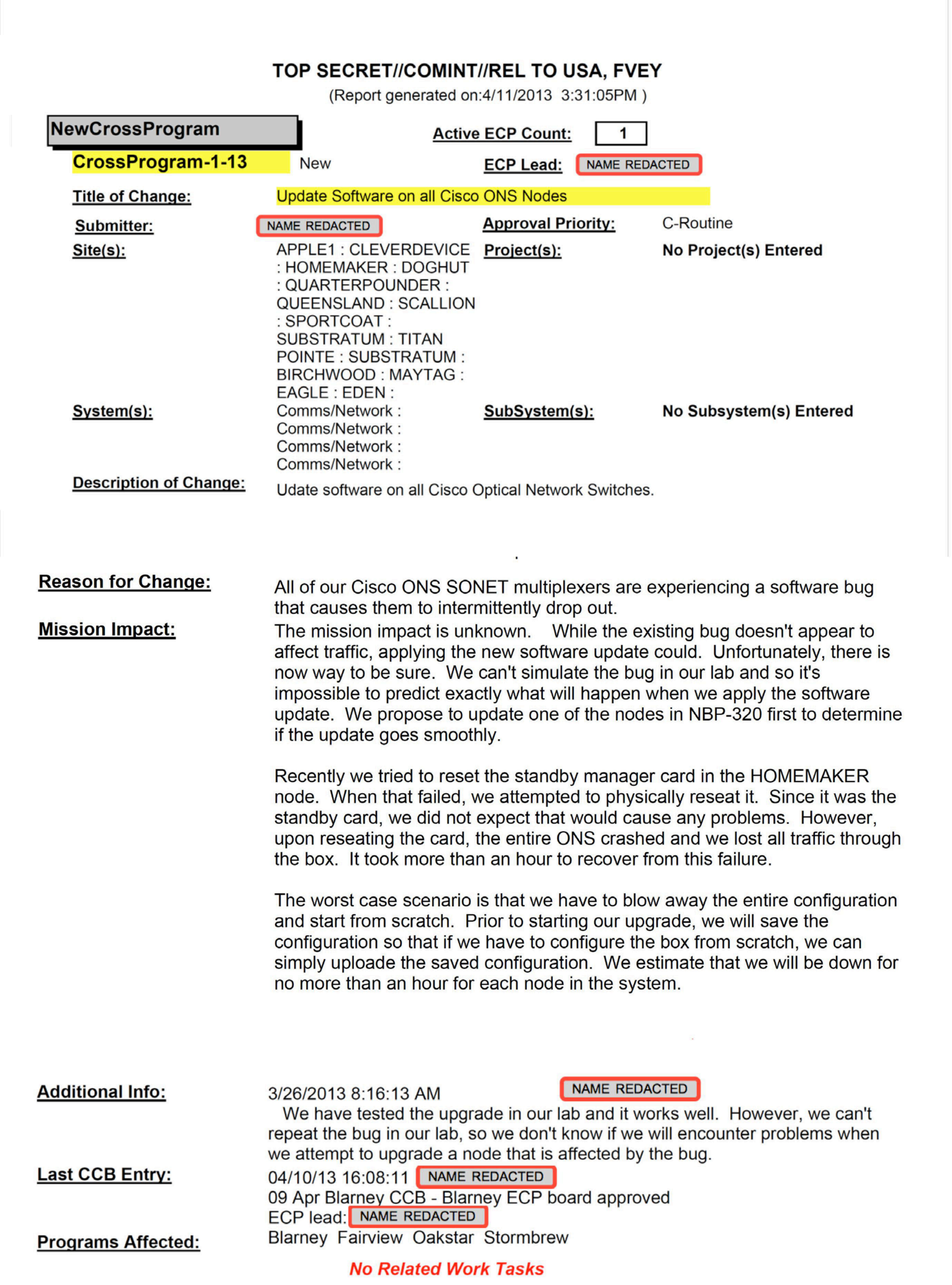
(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.



TOP SECRET//COMINT//REL TO USA, FVEY

(Report generated on:4/11/2013 3:31:05PM)

NewCrossProgram

Active ECP Count: 1

CrossProgram-1-13 New

ECP Lead: NAME REDACTED

Title of Change: Update Software on all Cisco ONS Nodes

Submitter: NAME REDACTED

Approval Priority: C-Routine

Site(s): APPLE1 : CLEVERDEVICE : HOMEMAKER : DOGHUT : QUARTERPOUNDER : QUEENSLAND : SCALLION : SPORTCOAT : SUBSTRATUM : TITAN POINTE : SUBSTRATUM : BIRCHWOOD : MAYTAG : EAGLE : EDEN :

Project(s): **No Project(s) Entered**

System(s): Comms/Network : Comms/Network : Comms/Network : Comms/Network :

SubSystem(s): **No Subsystem(s) Entered**

Description of Change: Udate software on all Cisco Optical Network Switches.

Reason for Change: All of our Cisco ONS SONET multiplexers are experiencing a software bug that causes them to intermittently drop out.

Mission Impact: The mission impact is unknown. While the existing bug doesn't appear to affect traffic, applying the new software update could. Unfortunately, there is now way to be sure. We can't simulate the bug in our lab and so it's impossible to predict exactly what will happen when we apply the software update. We propose to update one of the nodes in NBP-320 first to determine if the update goes smoothly.

Recently we tried to reset the standby manager card in the HOMEMAKER node. When that failed, we attempted to physically reseat it. Since it was the standby card, we did not expect that would cause any problems. However, upon reseating the card, the entire ONS crashed and we lost all traffic through the box. It took more than an hour to recover from this failure.

The worst case scenario is that we have to blow away the entire configuration and start from scratch. Prior to starting our upgrade, we will save the configuration so that if we have to configure the box from scratch, we can simply uploade the saved configuration. We estimate that we will be down for no more than an hour for each node in the system.

Additional Info: 3/26/2013 8:16:13 AM NAME REDACTED

We have tested the upgrade in our lab and it works well. However, we can't repeat the bug in our lab, so we don't know if we will encounter problems when we attempt to upgrade a node that is affected by the bug.

Last CCB Entry: 04/10/13 16:08:11 NAME REDACTED

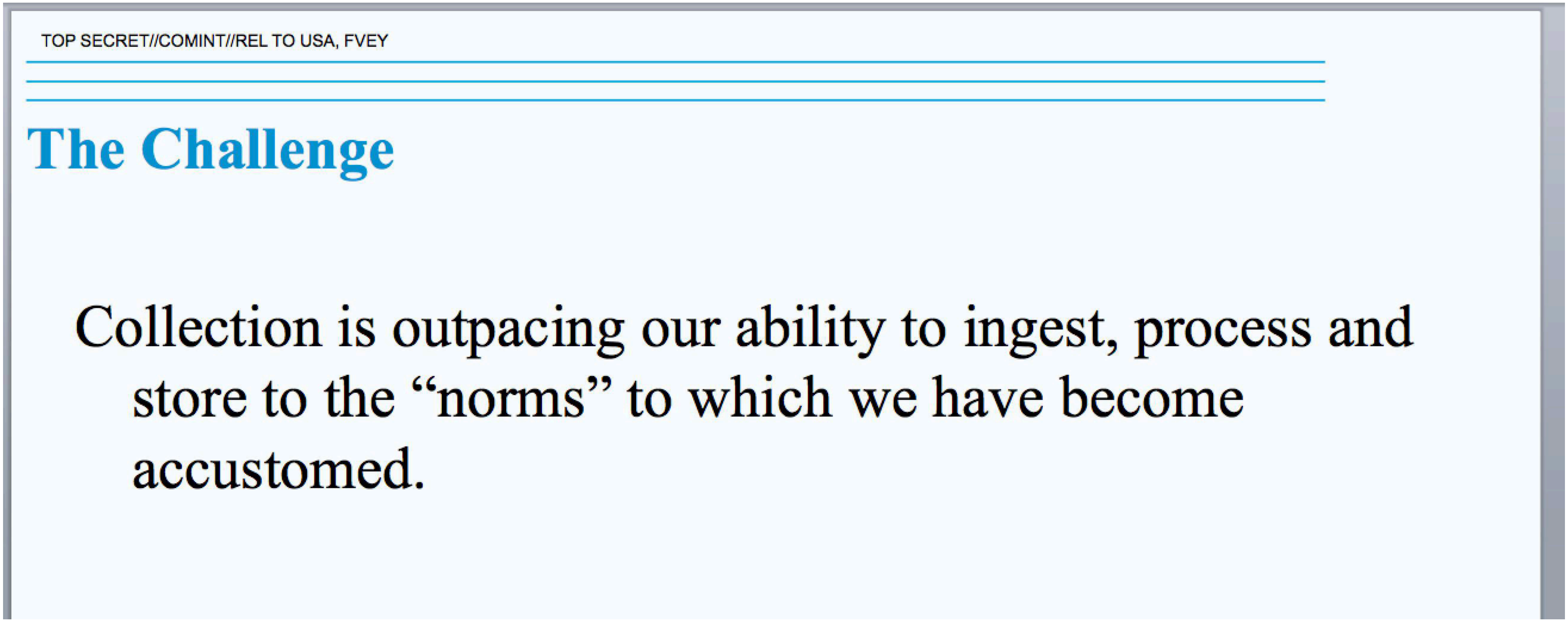
09 Apr Blarney CCB - Blarney ECP board approved

ECP lead: NAME REDACTED

Programs Affected: Blarney Fairview Oakstar Stormbrew

No Related Work Tasks

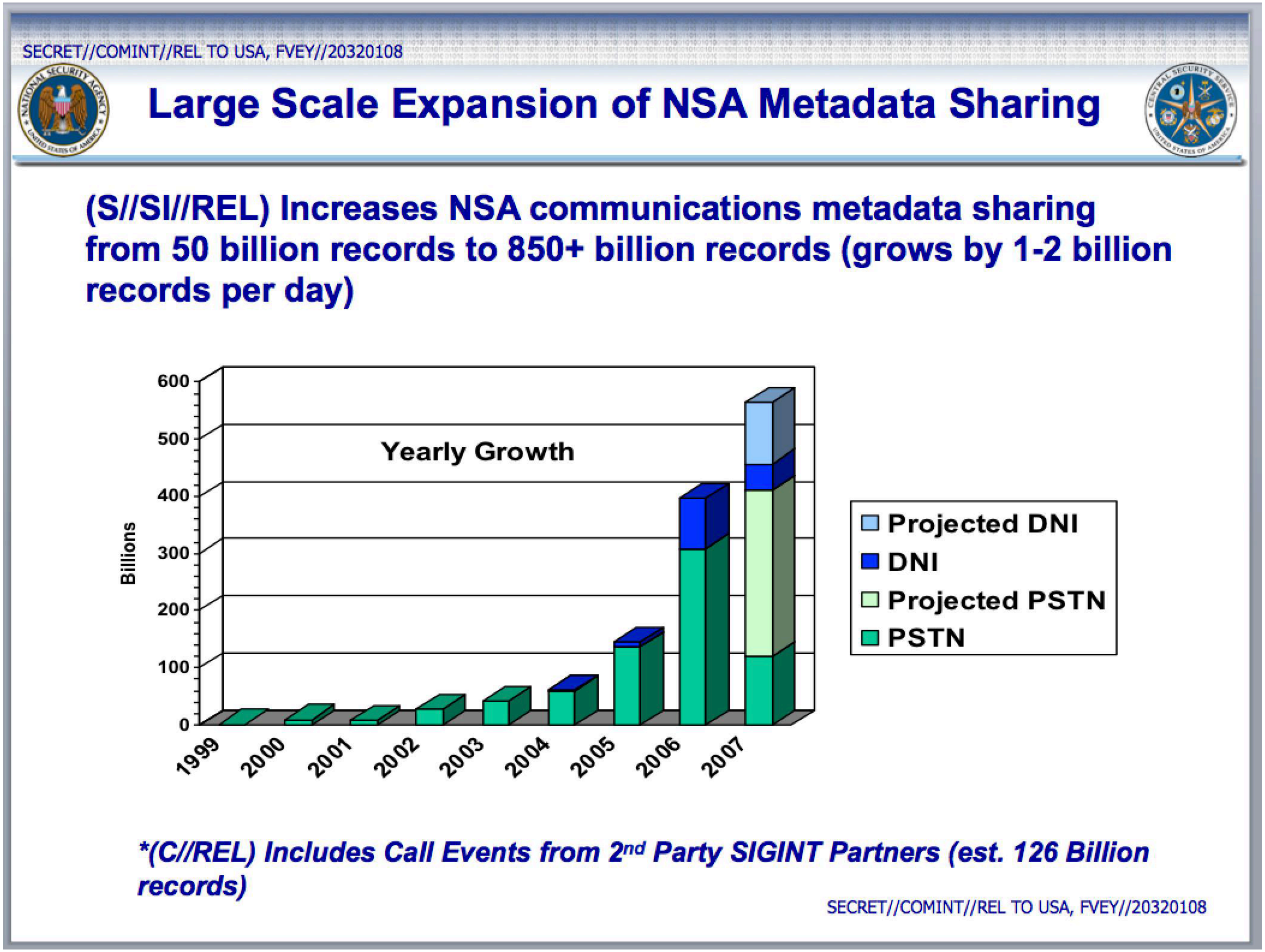
Page 151



TOP SECRET//COMINT//REL TO USA, FVEY

The Challenge

Collection is outpacing our ability to ingest, process and store to the "norms" to which we have become accustomed.



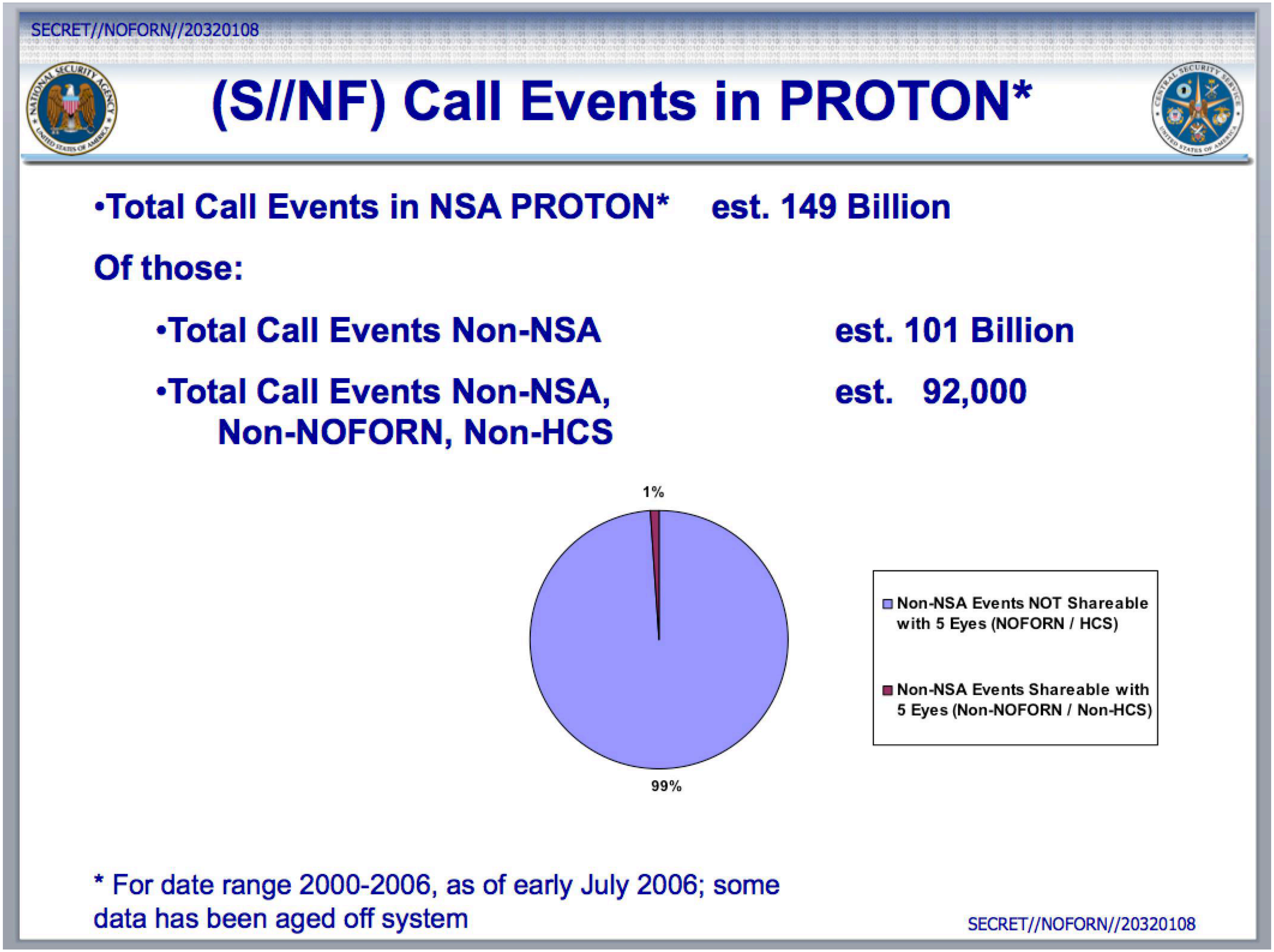
SECRET//COMINT//REL TO USA, FVEY//20320108

Large Scale Expansion of NSA Metadata Sharing

(S//SI//REL) Increases NSA communications metadata sharing from 50 billion records to 850+ billion records (grows by 1-2 billion records per day)

(C//REL) Includes Call Events from 2nd Party SIGINT Partners (est. 126 Billion records)

SECRET//COMINT//REL TO USA, FVEY//20320108



SECRET//NOFORN//20320108

(S//NF) Call Events in PROTON*

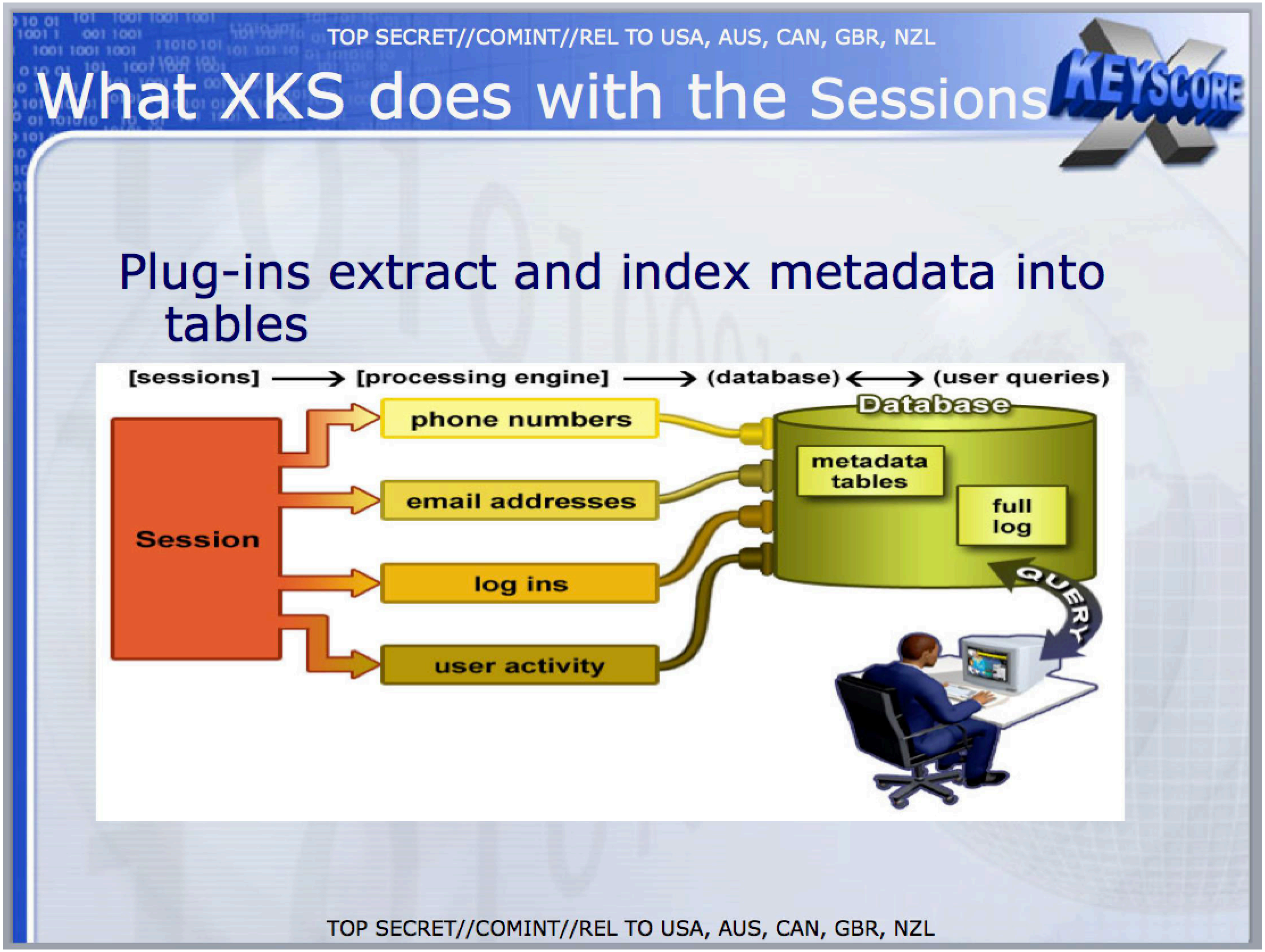
- Total Call Events in NSA PROTON* est. 149 Billion

Of those:

- Total Call Events Non-NSA est. 101 Billion
- Total Call Events Non-NSA, Non-NOFORN, Non-HCS est. 92,000

* For date range 2000-2006, as of early July 2006; some data has been aged off system

SECRET//NOFORN//20320108



What XKS does with the Sessions

Plug-ins extract and index metadata into tables

[sessions] → [processing engine] → (database) ↔ (user queries)

Session

phone numbers

email addresses

log ins

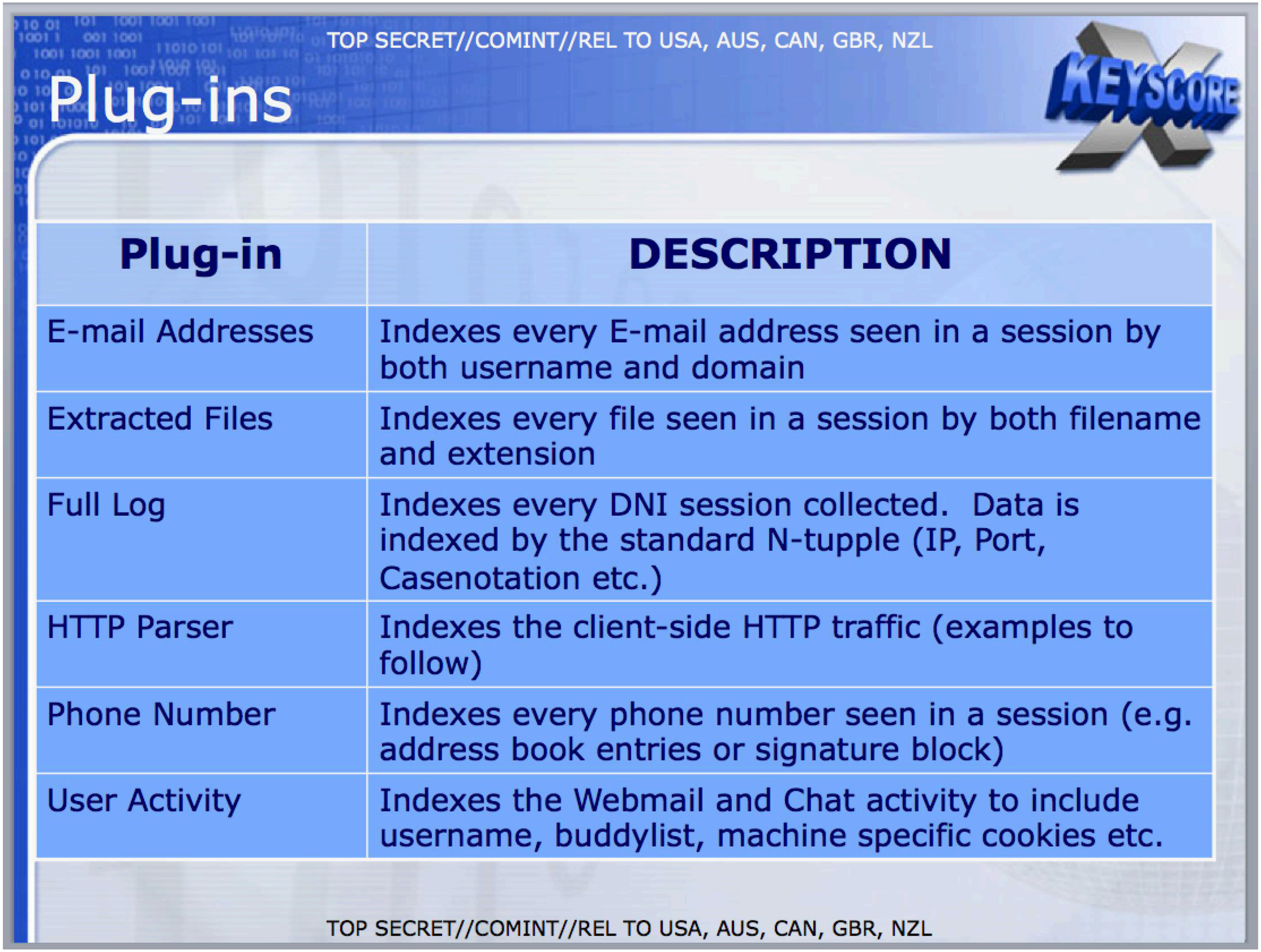
user activity

Database

metadata tables

full log

QUERY

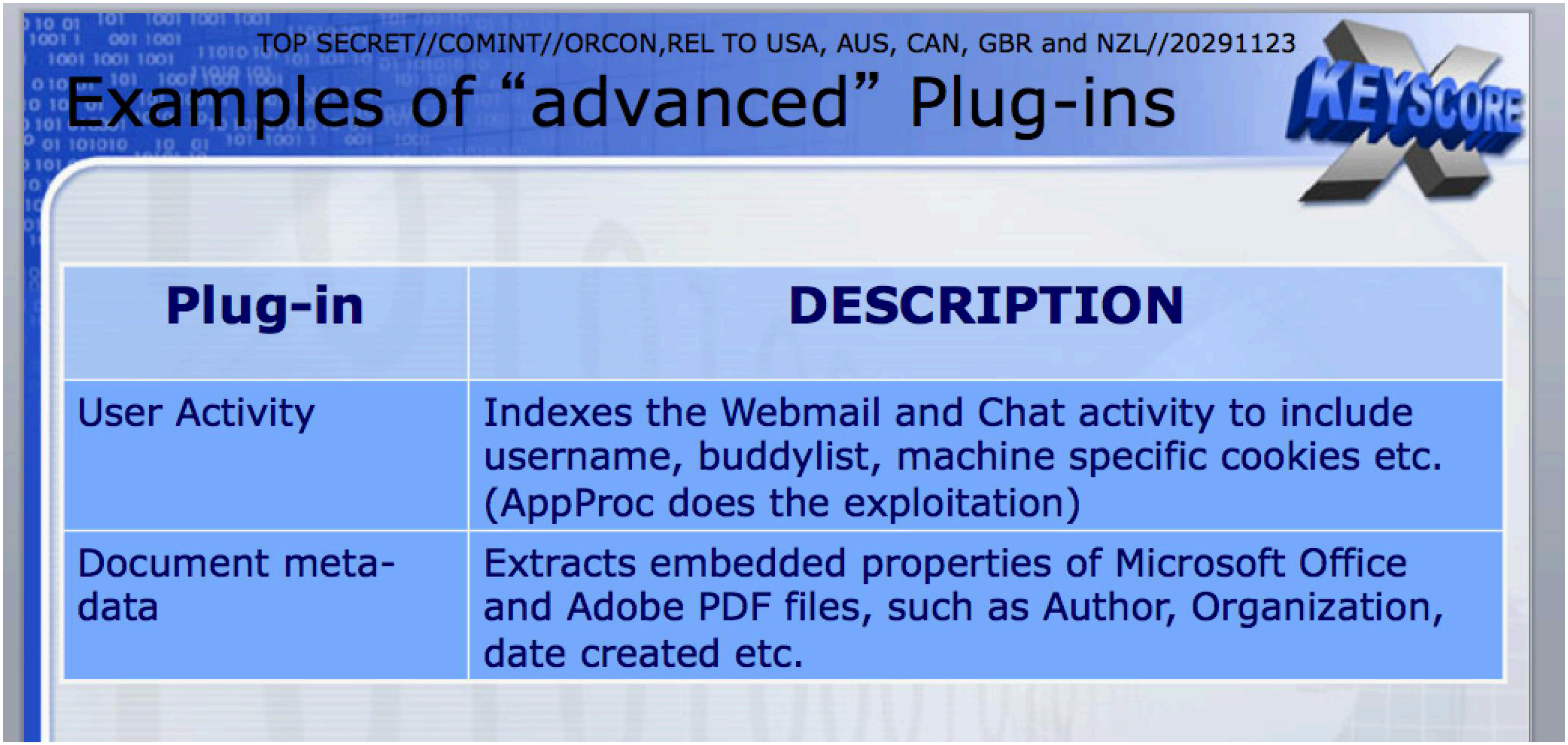


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

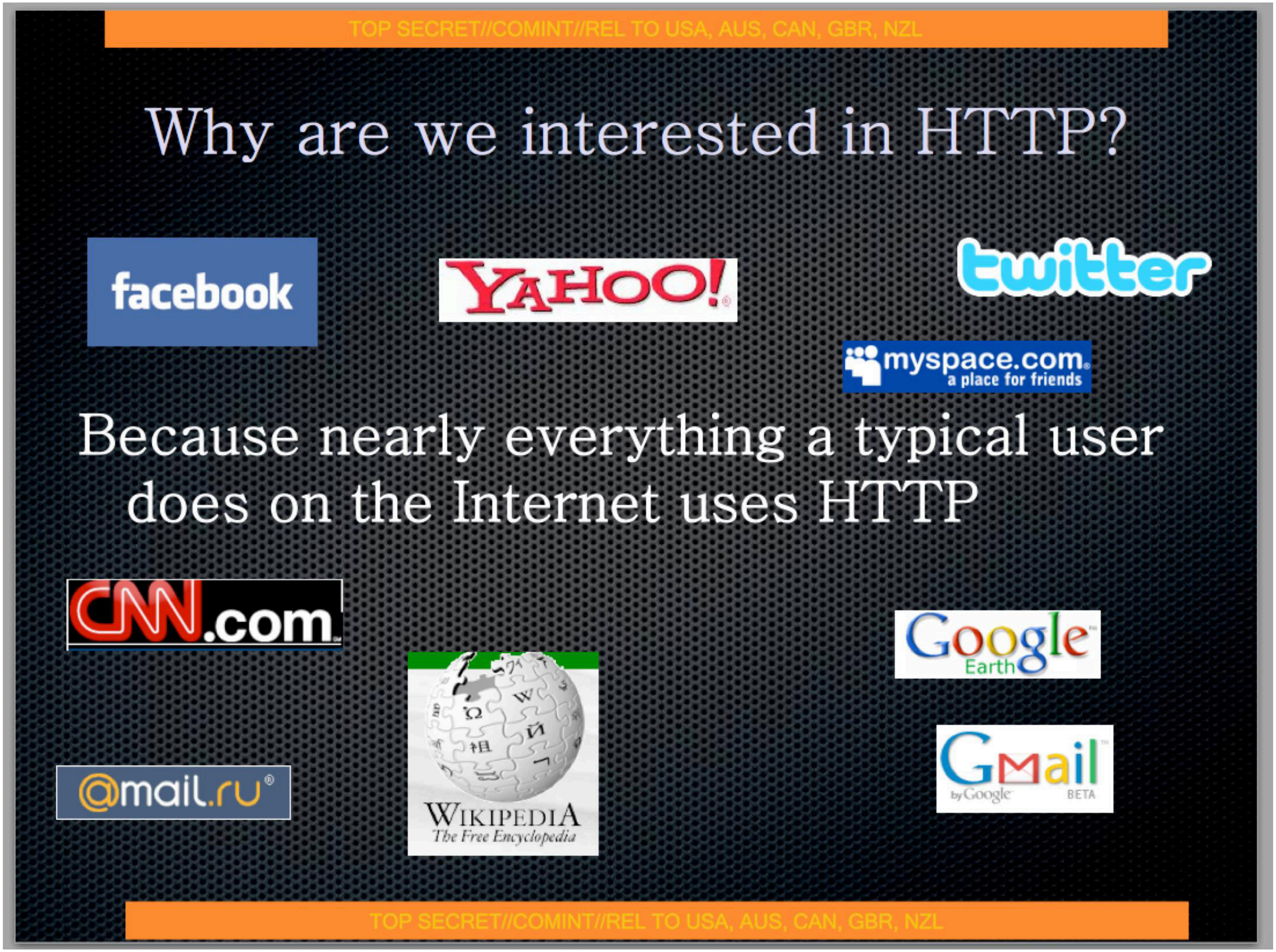
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

Examples of “advanced” Plug-ins

Plug-in	DESCRIPTION
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. (AppProc does the exploitation)
Document meta-data	Extracts embedded properties of Microsoft Office and Adobe PDF files, such as Author, Organization, date created etc.



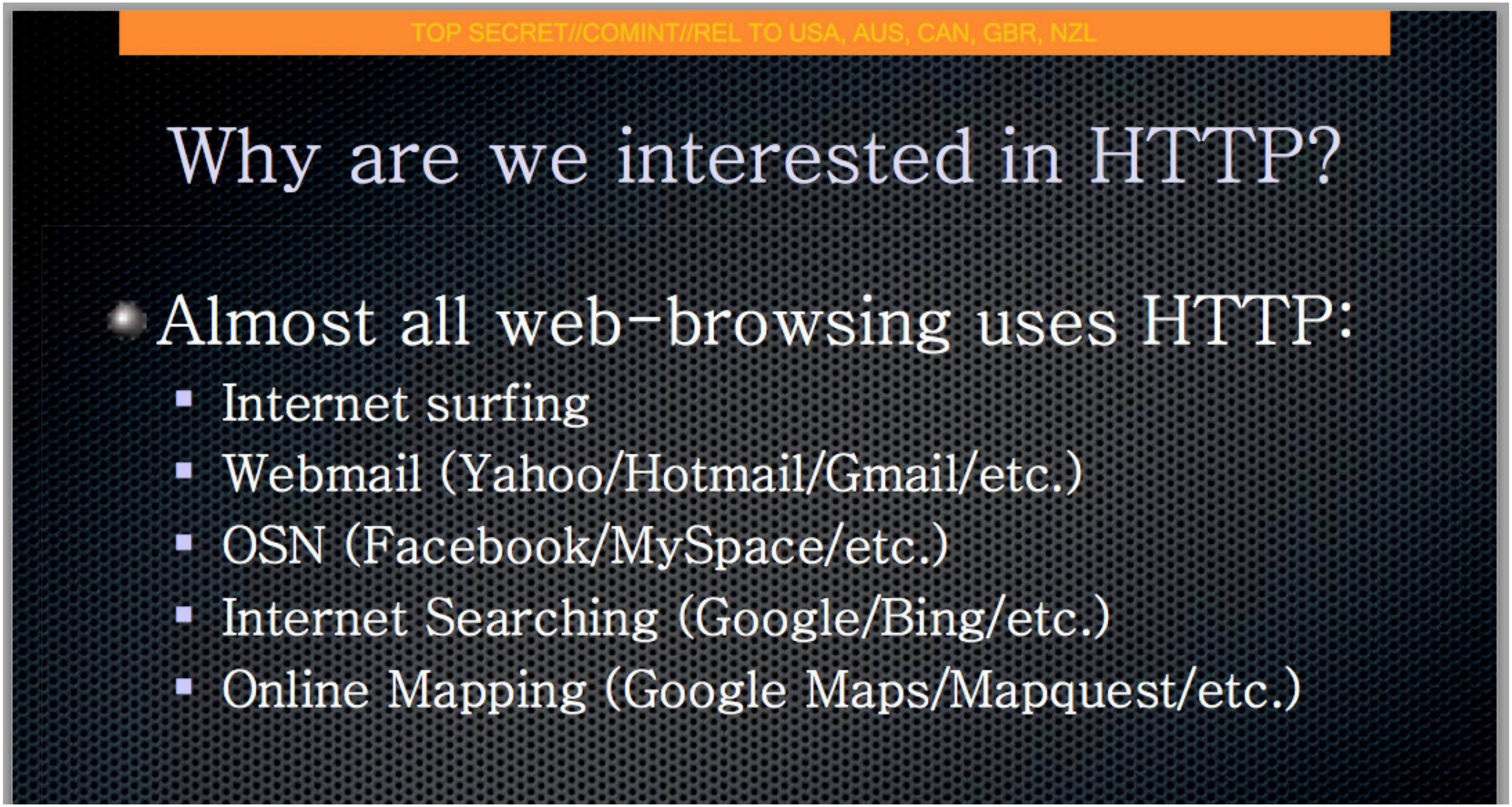
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Why are we interested in HTTP?

Because nearly everything a typical user does on the Internet uses HTTP

facebook
YAHOO!
twitter
myspace.com
a place for friends
CNN.com
@mail.ru
WIKIPEDIA
The Free Encyclopedia
Google Earth
GMail
by Google
BETA

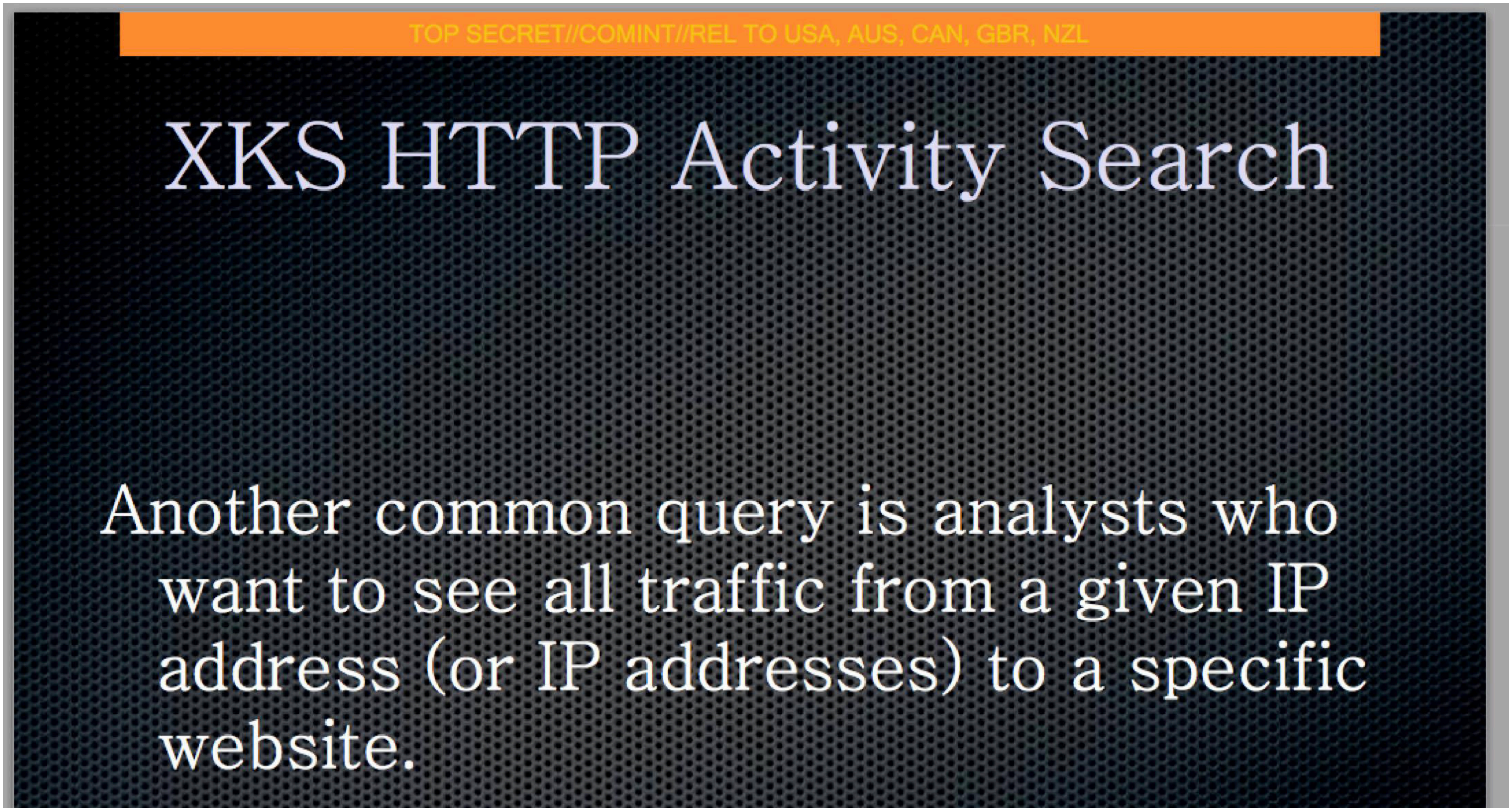
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Why are we interested in HTTP?

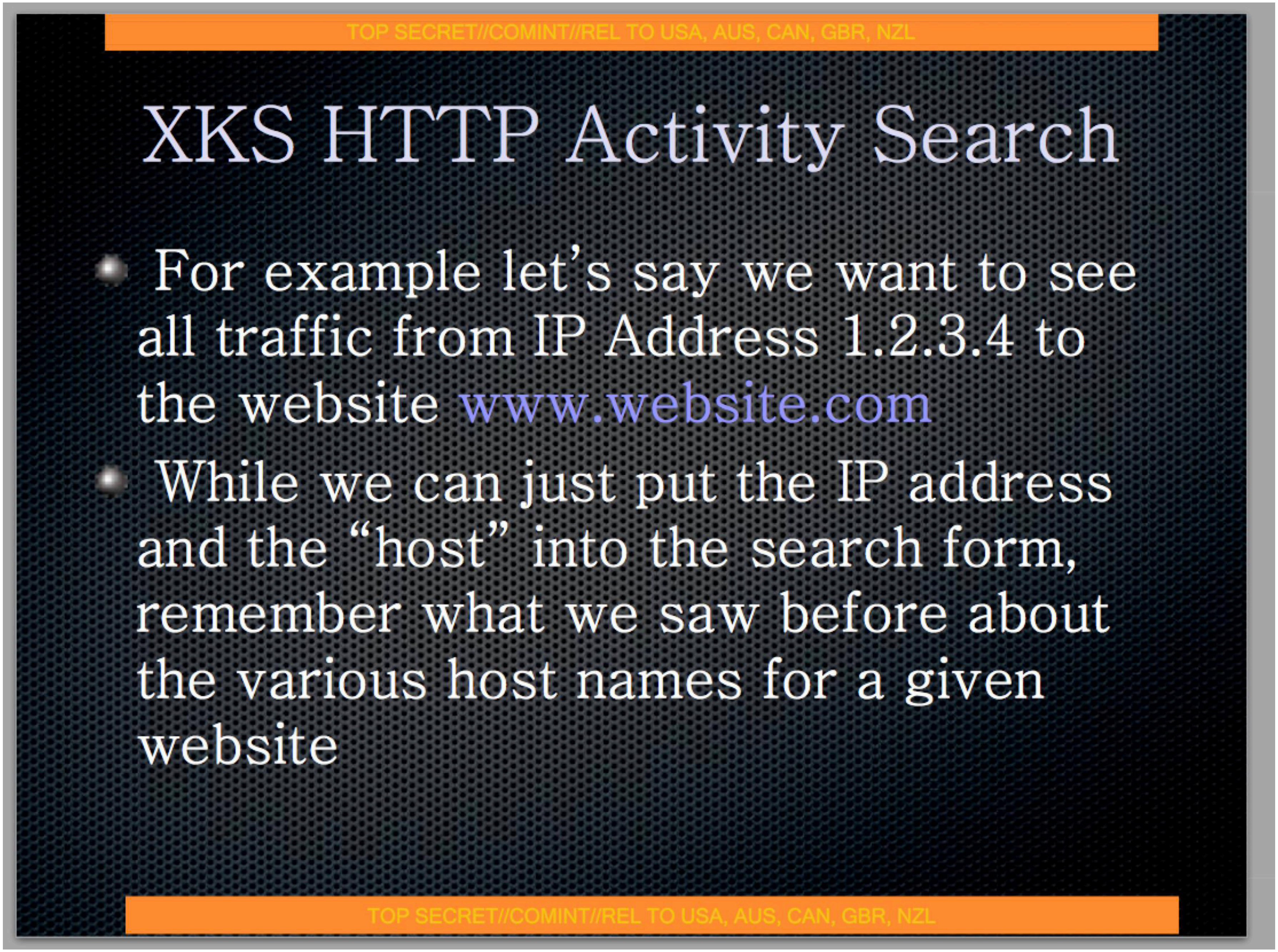
- Almost all web-browsing uses HTTP:
  - Internet surfing
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Internet Searching (Google/Bing/etc.)
  - Online Mapping (Google Maps/Mapquest/etc.)



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKS HTTP Activity Search

Another common query is analysts who want to see all traffic from a given IP address (or IP addresses) to a specific website.

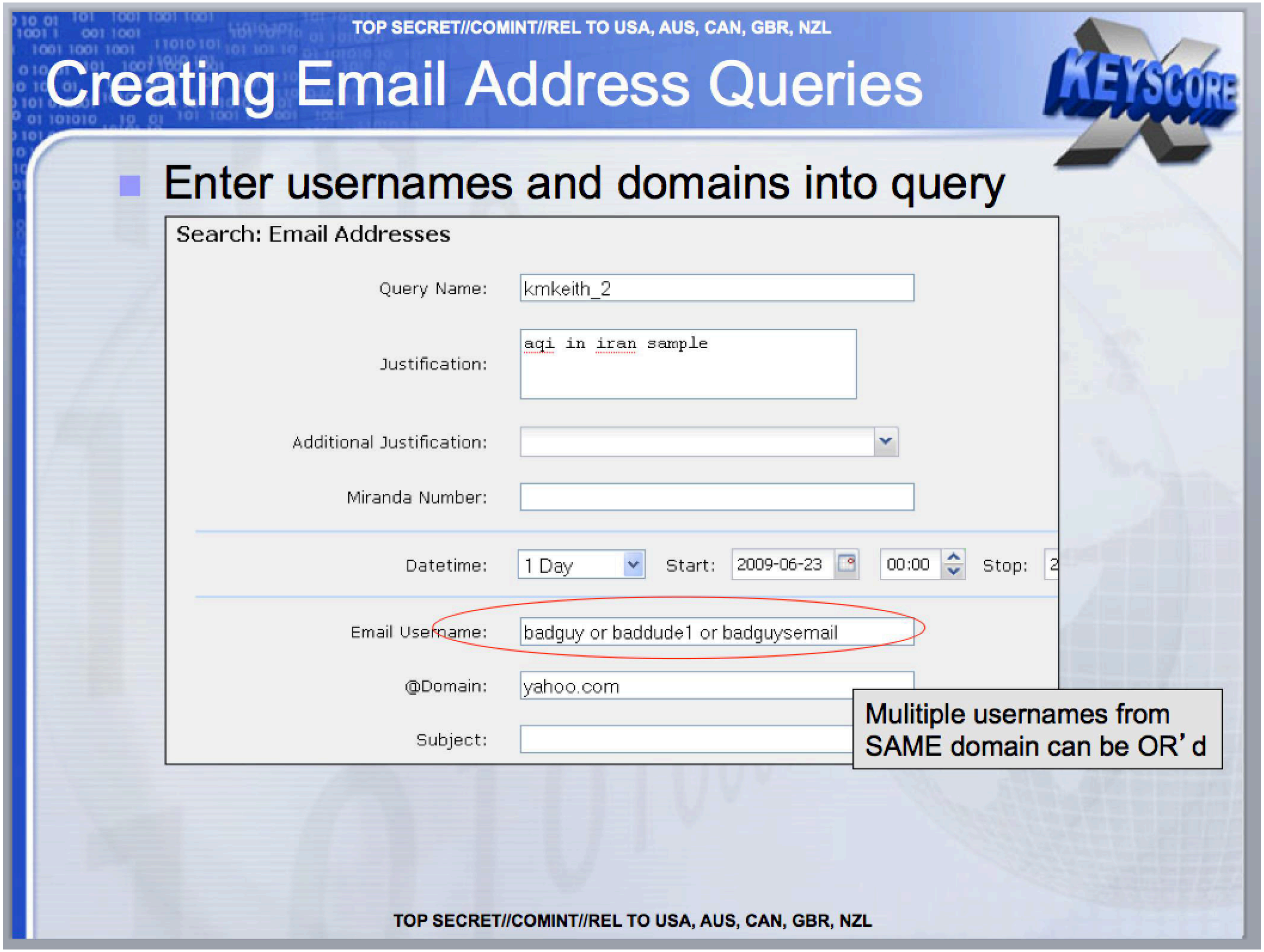


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKS HTTP Activity Search

- For example let's say we want to see all traffic from IP Address 1.2.3.4 to the website www.website.com
- While we can just put the IP address and the "host" into the search form, remember what we saw before about the various host names for a given website

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Creating Email Address Queries

- Enter usernames and domains into query

Search: Email Addresses

Query Name: kmkeith_2

Justification: aqi in iran sample

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-06-23 00:00 Stop: 2

Email Username: badguy or baddude1 or badguysemail

@Domain: yahoo.com

Subject:

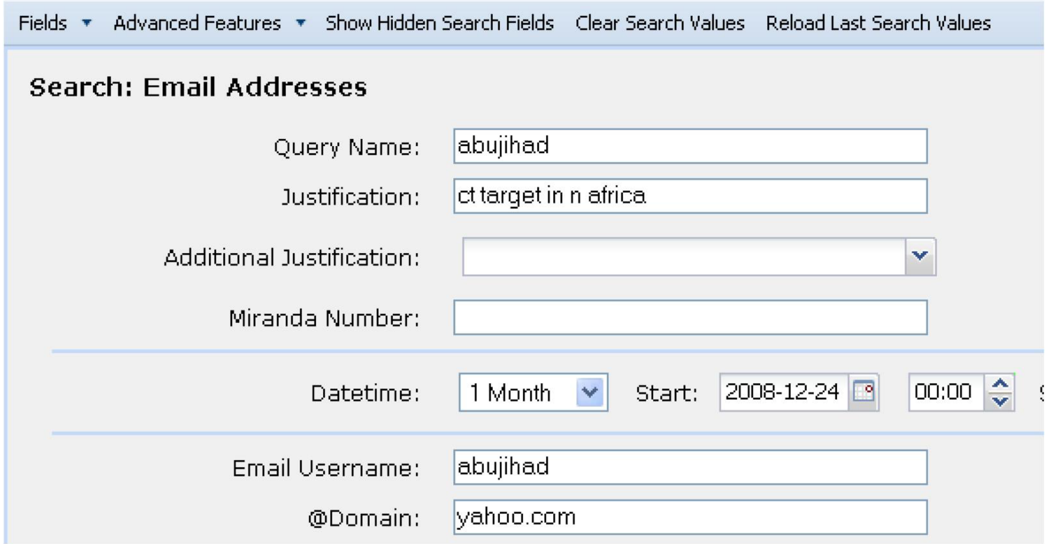
Mulitiple usernames from SAME domain can be OR’ d

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Email Addresses Query:

One of the most common queries is (you guessed it) an **Email Address Query** searching for an email address. To create a query for a specific email address, you have to fill in the name of the query, justify it and set a date range then you simply fill in the email address(es) you want to search on and submit.

That would look something like this…



Search: Email Addresses

Query Name: abujihad

Justification: ct target in n africa

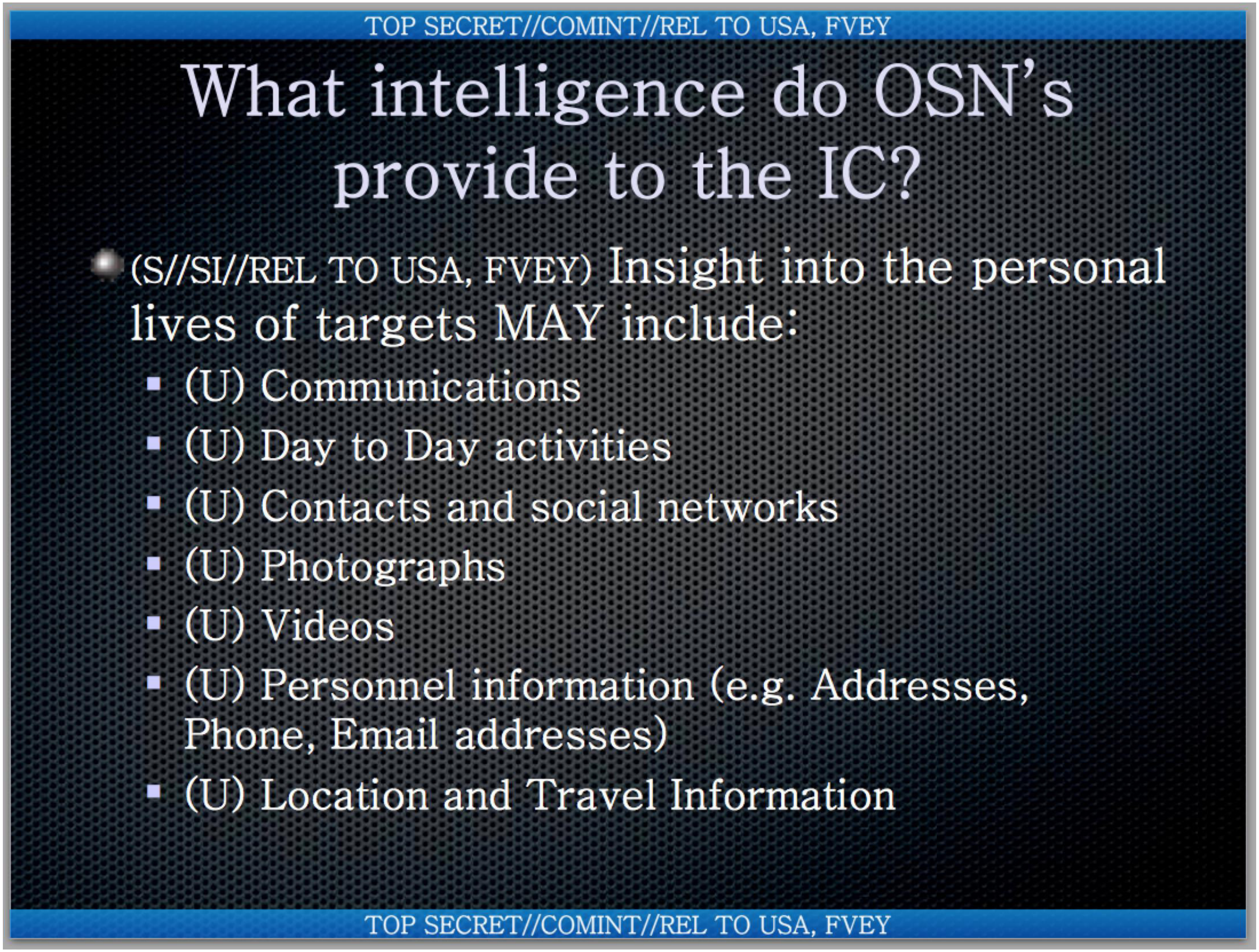
Additional Justification:

Miranda Number:

Datetime: 1 Month Start: 2008-12-24 00:00

Email Username: abujihad

@Domain: yahoo.com

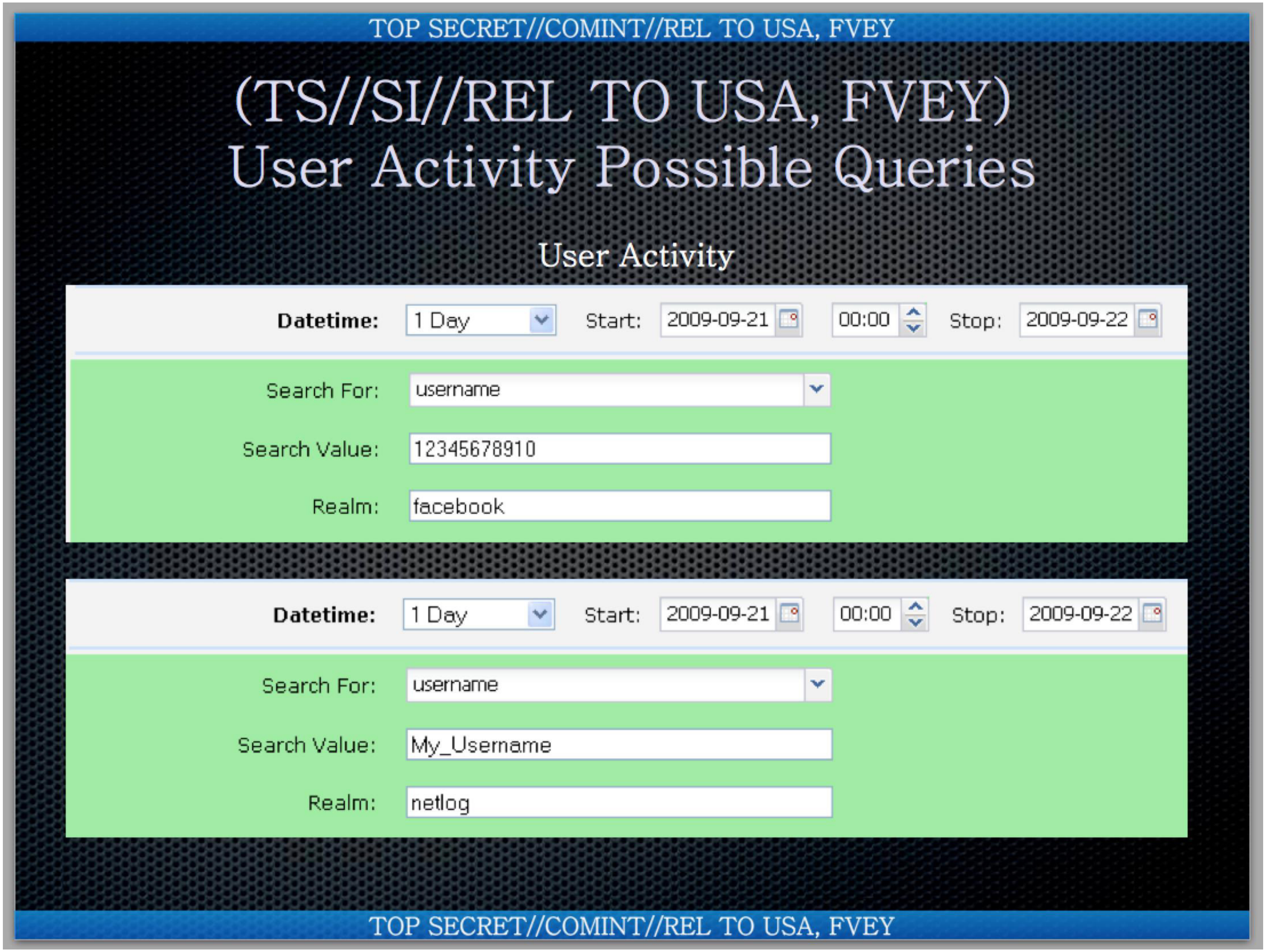


TOP SECRET//COMINT//REL TO USA, FVEY

What intelligence do OSN's provide to the IC?

- (S//SI//REL TO USA, FVEY) Insight into the personal lives of targets MAY include:
  - (U) Communications
  - (U) Day to Day activities
  - (U) Contacts and social networks
  - (U) Photographs
  - (U) Videos
  - (U) Personnel information (e.g. Addresses, Phone, Email addresses)
  - (U) Location and Travel Information

TOP SECRET//COMINT//REL TO USA, FVEY



TOP SECRET//COMINT//REL TO USA, FVEY

(TS//SI//REL TO USA, FVEY) User Activity Possible Queries

User Activity

Datetime: 1 Day Start: 2009-09-21 00:00 Stop: 2009-09-22

Search For: username

Search Value: 12345678910

Realm: facebook

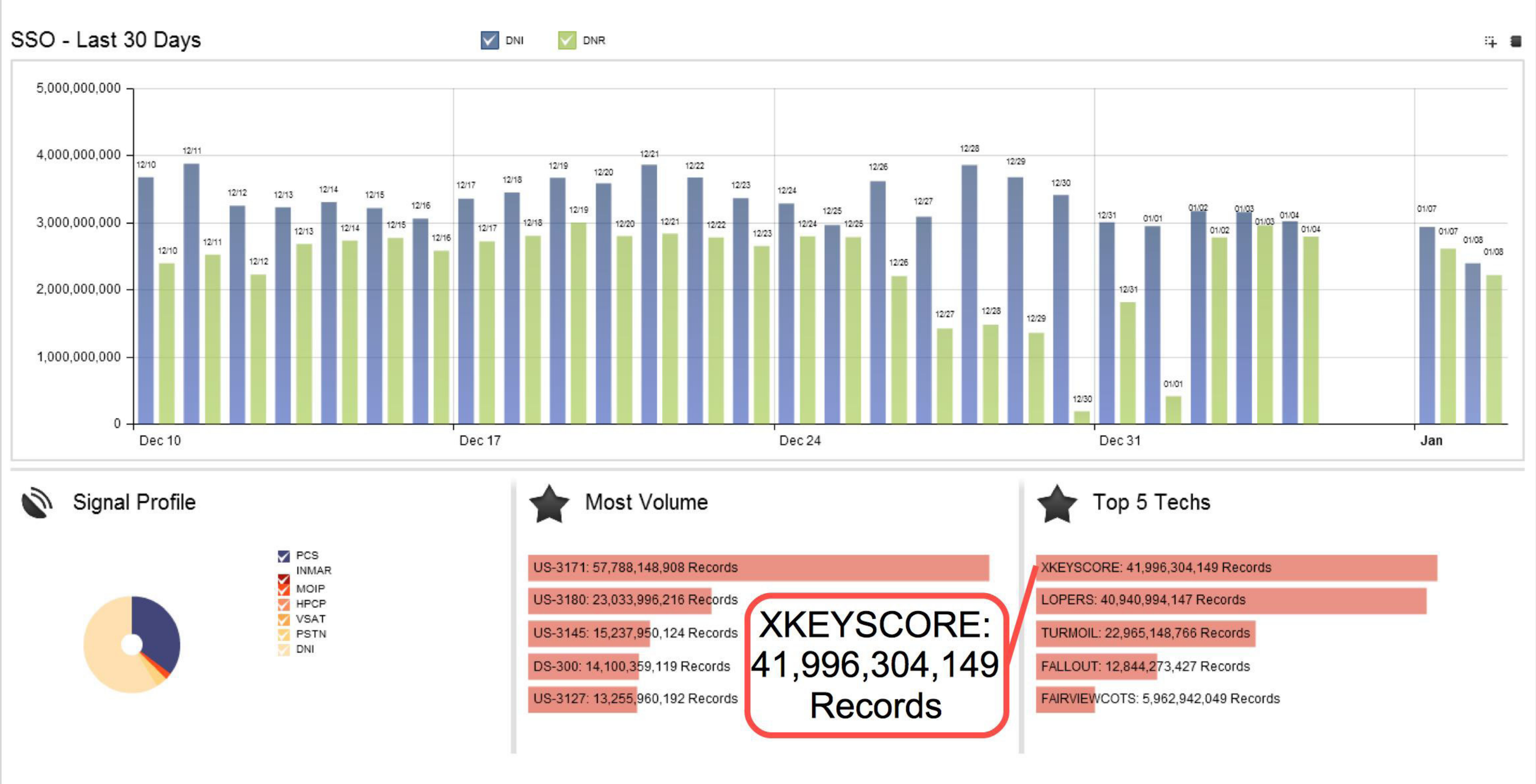
Datetime: 1 Day Start: 2009-09-21 00:00 Stop: 2009-09-22

Search For: username

Search Value: My_Username

Realm: netlog

TOP SECRET//COMINT//REL TO USA, FVEY



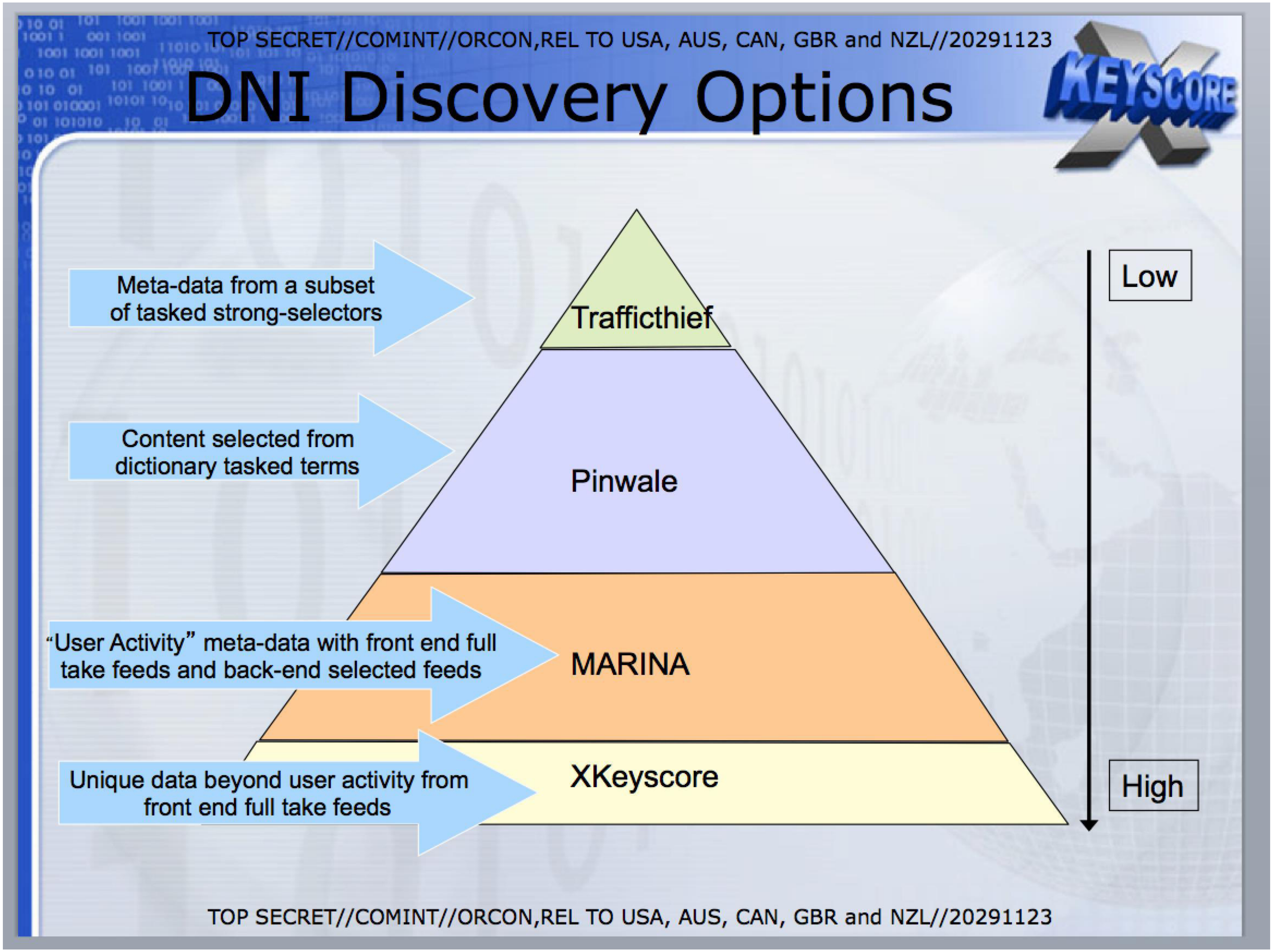
Most Volume

- US-3171: 57,788,148,908 Records
- US-3180: 23,033,996,216 Records
- US-3145: 15,237,950,124 Records
- DS-300: 14,100,359,119 Records
- US-3127: 13,255,960,192 Records

Top 5 Techs

- XKEYSCORE: 41,996,304,149 Records
- LOPERS: 40,940,994,147 Records
- TURMOIL: 22,965,148,766 Records
- FALLOUT: 12,844,273,427 Records
- FAIRVIEWCOTS: 5,962,942,049 Records

XKEYSCORE: 41,996,304,149 Records



TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

DNI Discovery Options

Meta-data from a subset of tasked strong-selectors

Traffícthief

Content selected from dictionary tasked terms

Pinwale

“User Activity” meta-data with front end full take feeds and back-end selected feeds

MARINA

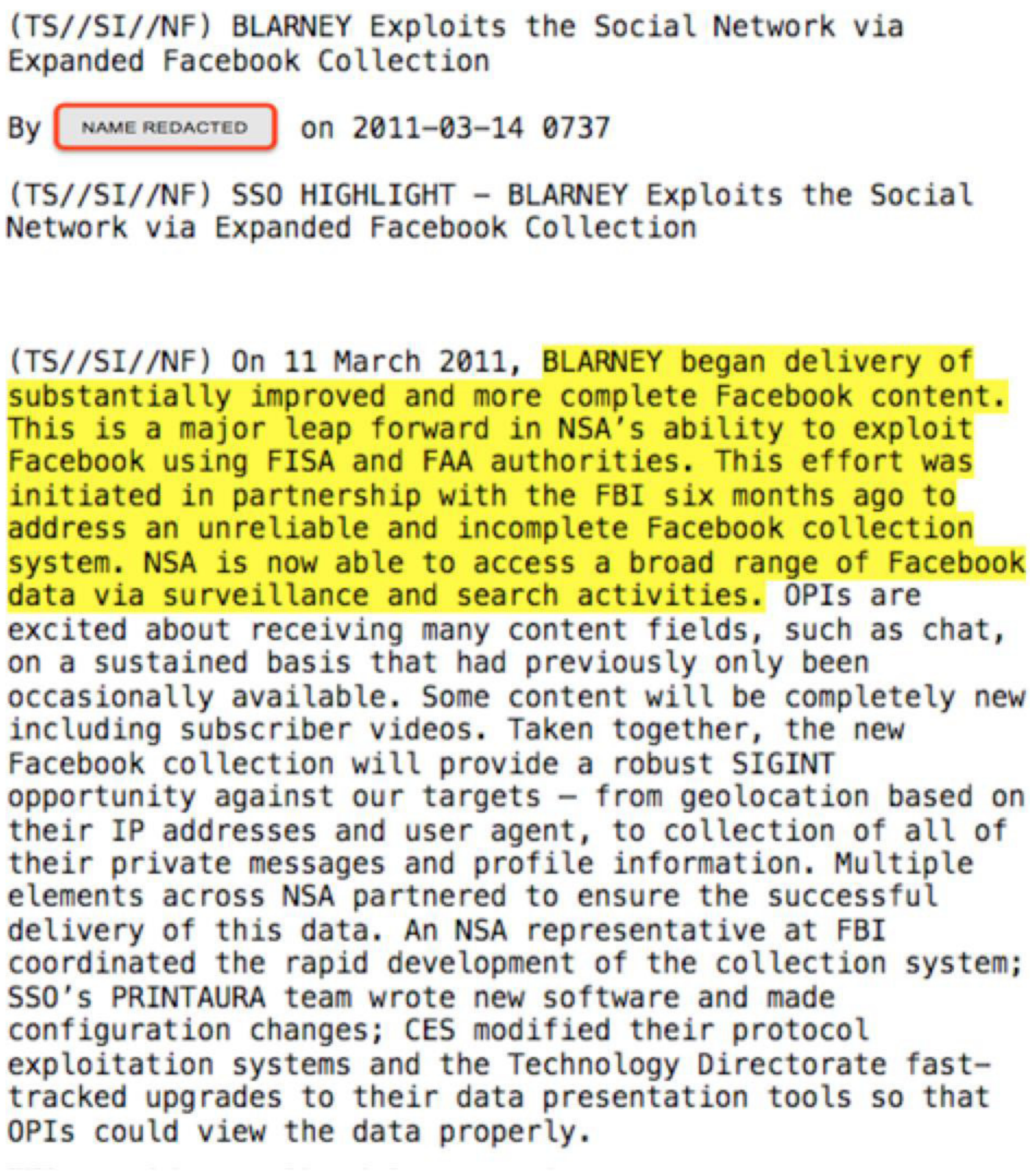
Unique data beyond user activity from front end full take feeds

XKeyscore

Low

High

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

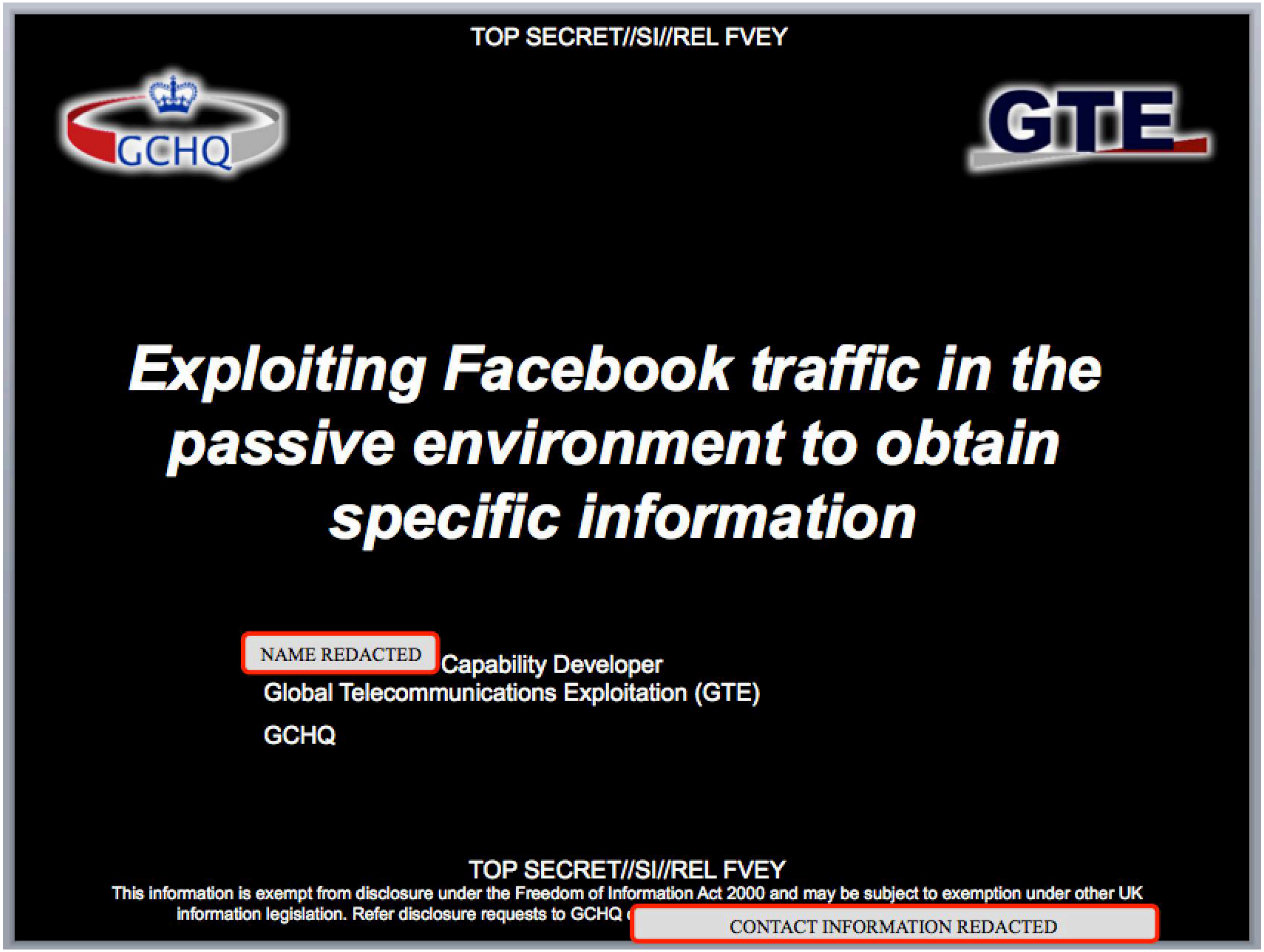


(TS//SI//NF) BLARNEY Exploits the Social Network via Expanded Facebook Collection

By NAME REDACTED on 2011-03-14 0737

(TS//SI//NF) SSO HIGHLIGHT - BLARNEY Exploits the Social Network via Expanded Facebook Collection

(TS//SI//NF) On 11 March 2011, BLARNEY began delivery of substantially improved and more complete Facebook content. This is a major leap forward in NSA's ability to exploit Facebook using FISA and FAA authorities. This effort was initiated in partnership with the FBI six months ago to address an unreliable and incomplete Facebook collection system. NSA is now able to access a broad range of Facebook data via surveillance and search activities. OPIs are excited about receiving many content fields, such as chat, on a sustained basis that had previously only been occasionally available. Some content will be completely new including subscriber videos. Taken together, the new Facebook collection will provide a robust SIGINT opportunity against our targets – from geolocation based on their IP addresses and user agent, to collection of all of their private messages and profile information. Multiple elements across NSA partnered to ensure the successful delivery of this data. An NSA representative at FBI coordinated the rapid development of the collection system; SSO's PRINTAURA team wrote new software and made configuration changes; CES modified their protocol exploitation systems and the Technology Directorate fast-tracked upgrades to their data presentation tools so that OPIs could view the data properly.



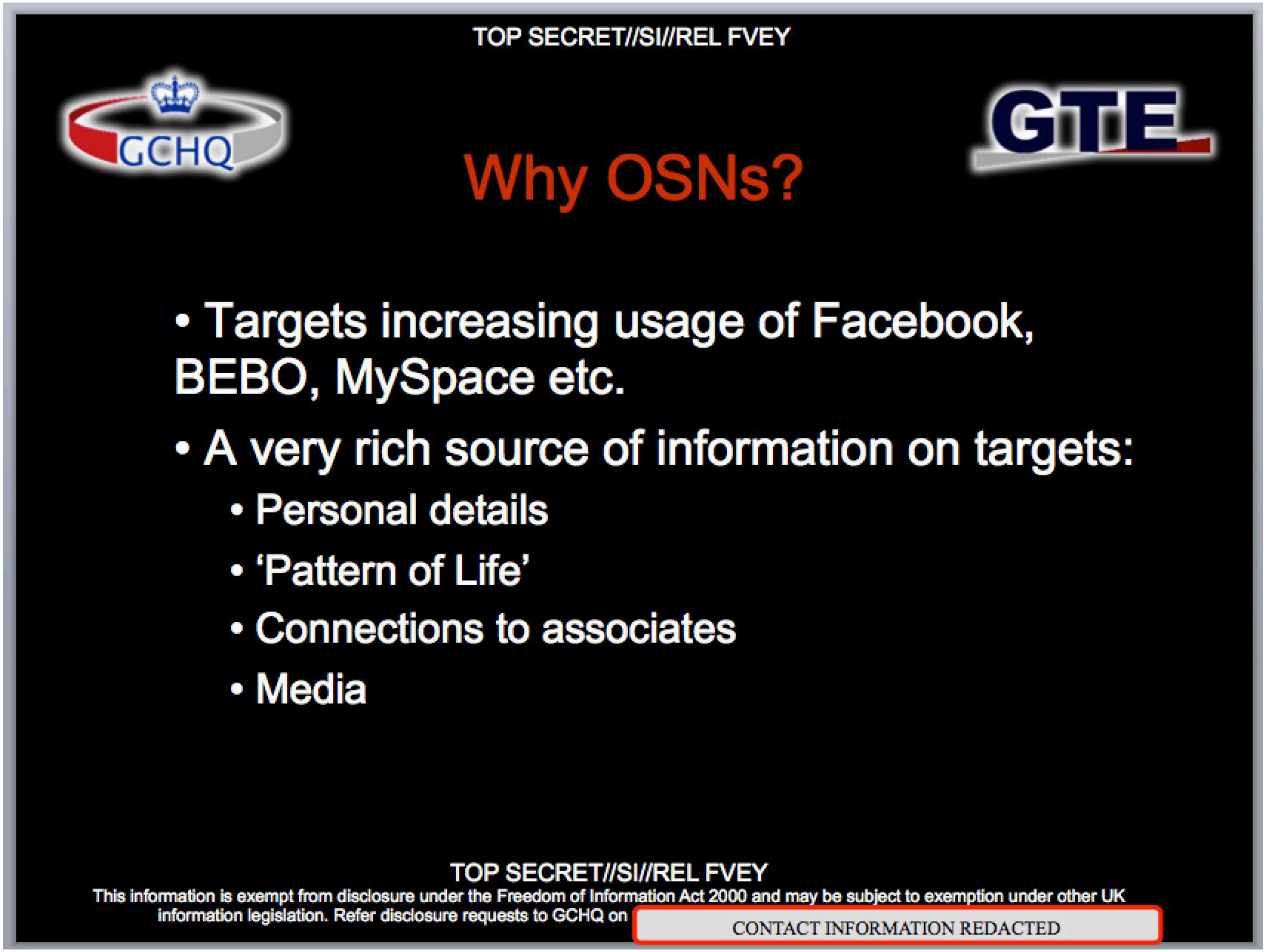
TOP SECRET//SI//REL FVEY

Exploiting Facebook traffic in the passive environment to obtain specific information

NAME REDACTED Capability Developer
Global Telecommunications Exploitation (GTE)
GCHQ

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ CONTACT INFORMATION REDACTED



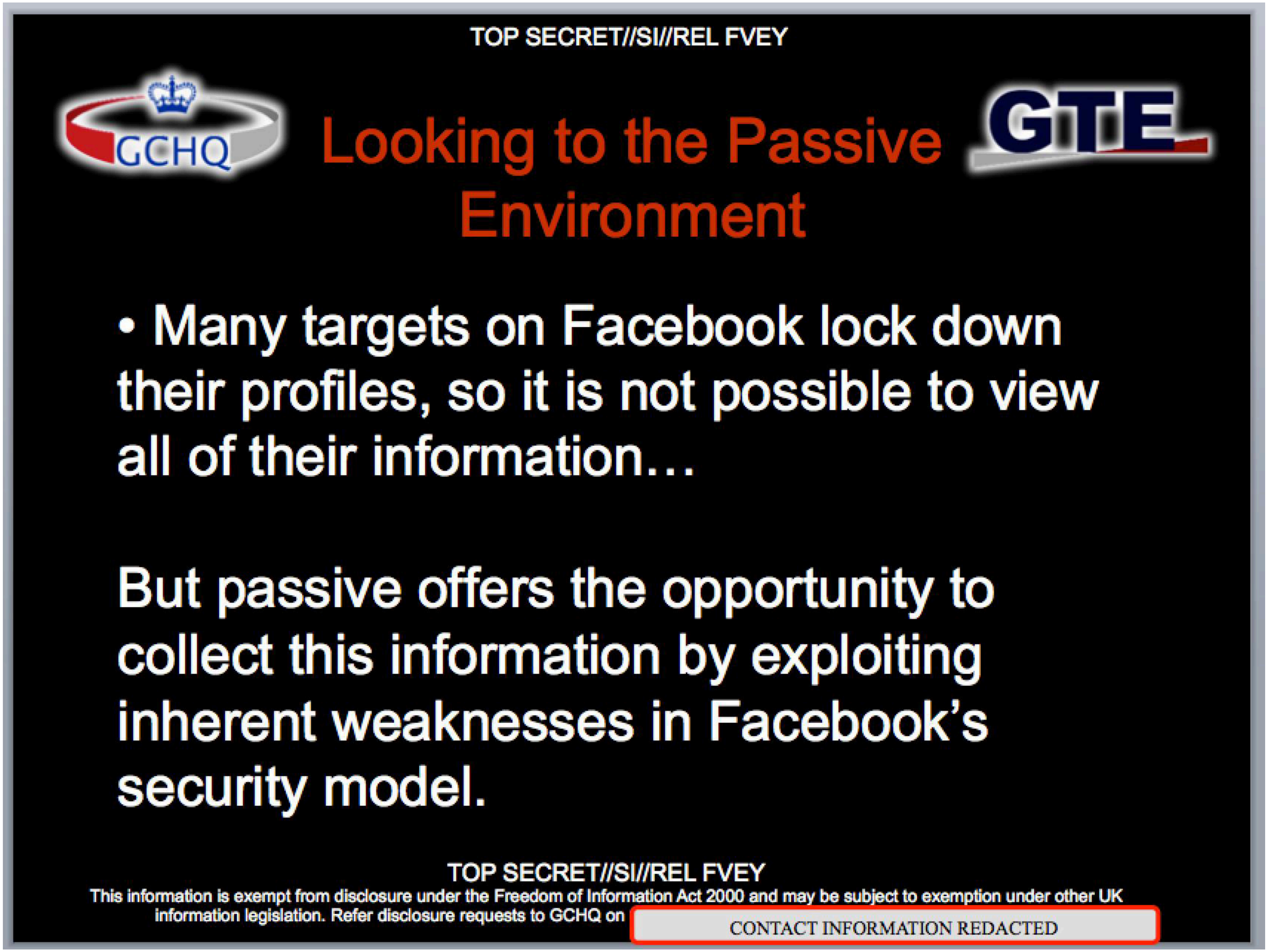
TOP SECRET//SI//REL FVEY

Why OSNs?

- Targets increasing usage of Facebook, BEBO, MySpace etc.
- A very rich source of information on targets:
  - Personal details
  - ‘Pattern of Life’
  - Connections to associates
  - Media

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

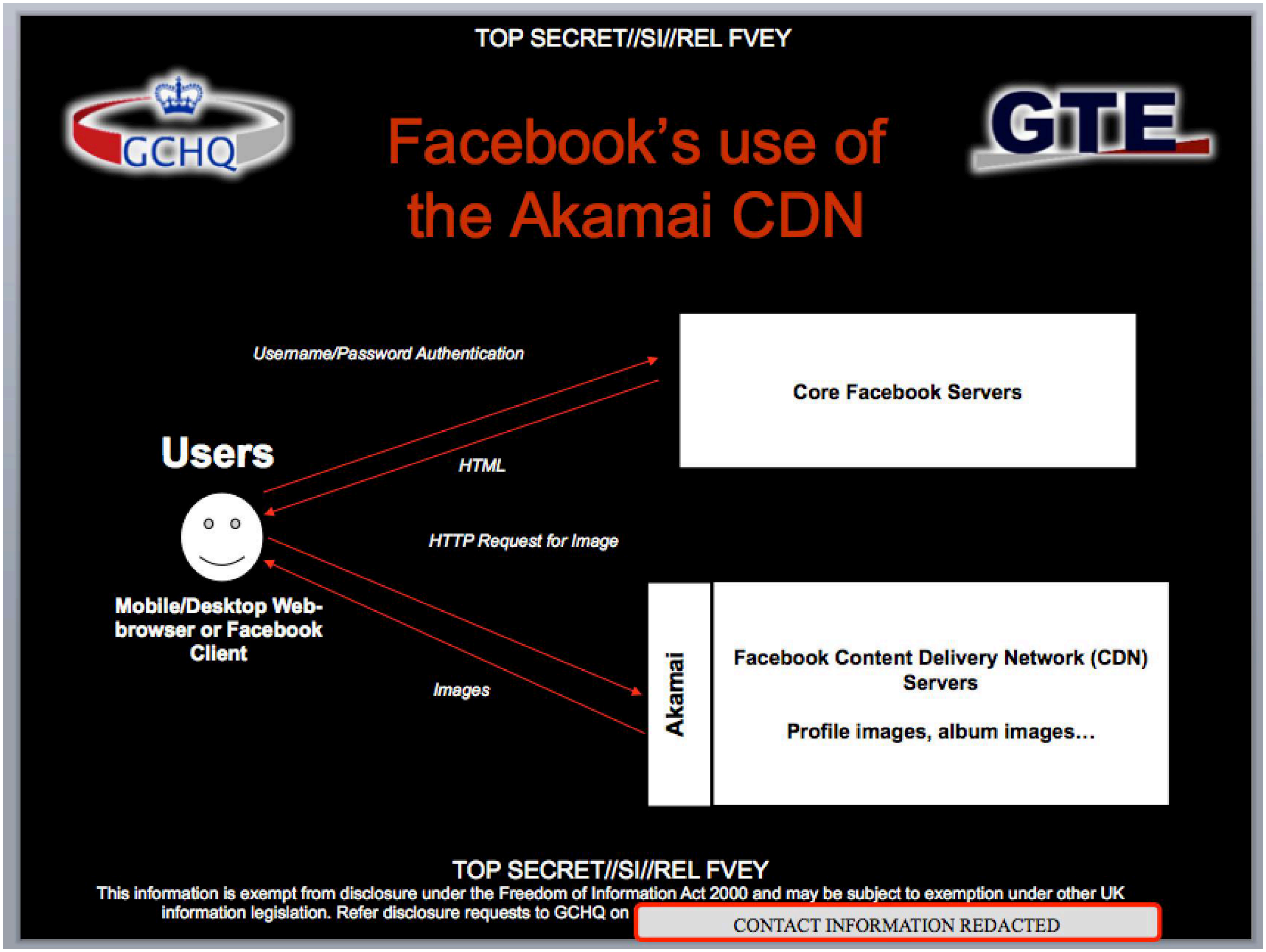
Looking to the Passive Environment

- Many targets on Facebook lock down their profiles, so it is not possible to view all of their information…

But passive offers the opportunity to collect this information by exploiting inherent weaknesses in Facebook's security model.

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

GCHQ

GTE

Facebook's use of the Akamai CDN

Username/Password Authentication

HTML

Core Facebook Servers

Users

Mobile/Desktop Web-browser or Facebook Client

HTTP Request for Image

Images

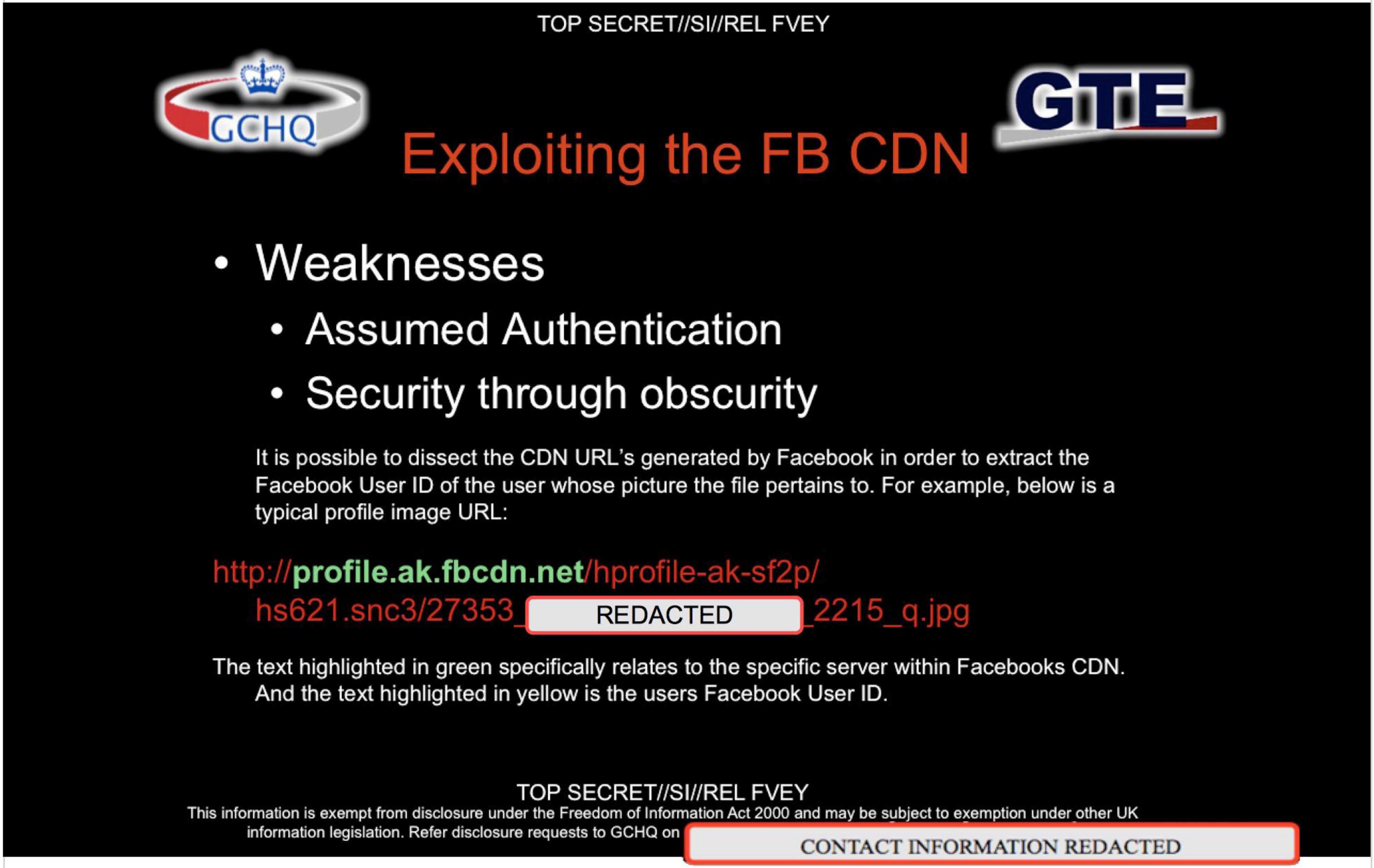
Akamai

Facebook Content Delivery Network (CDN) Servers

Profile images, album images…

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

Exploiting the FB CDN

- Weaknesses
  - Assumed Authentication
  - Security through obscurity

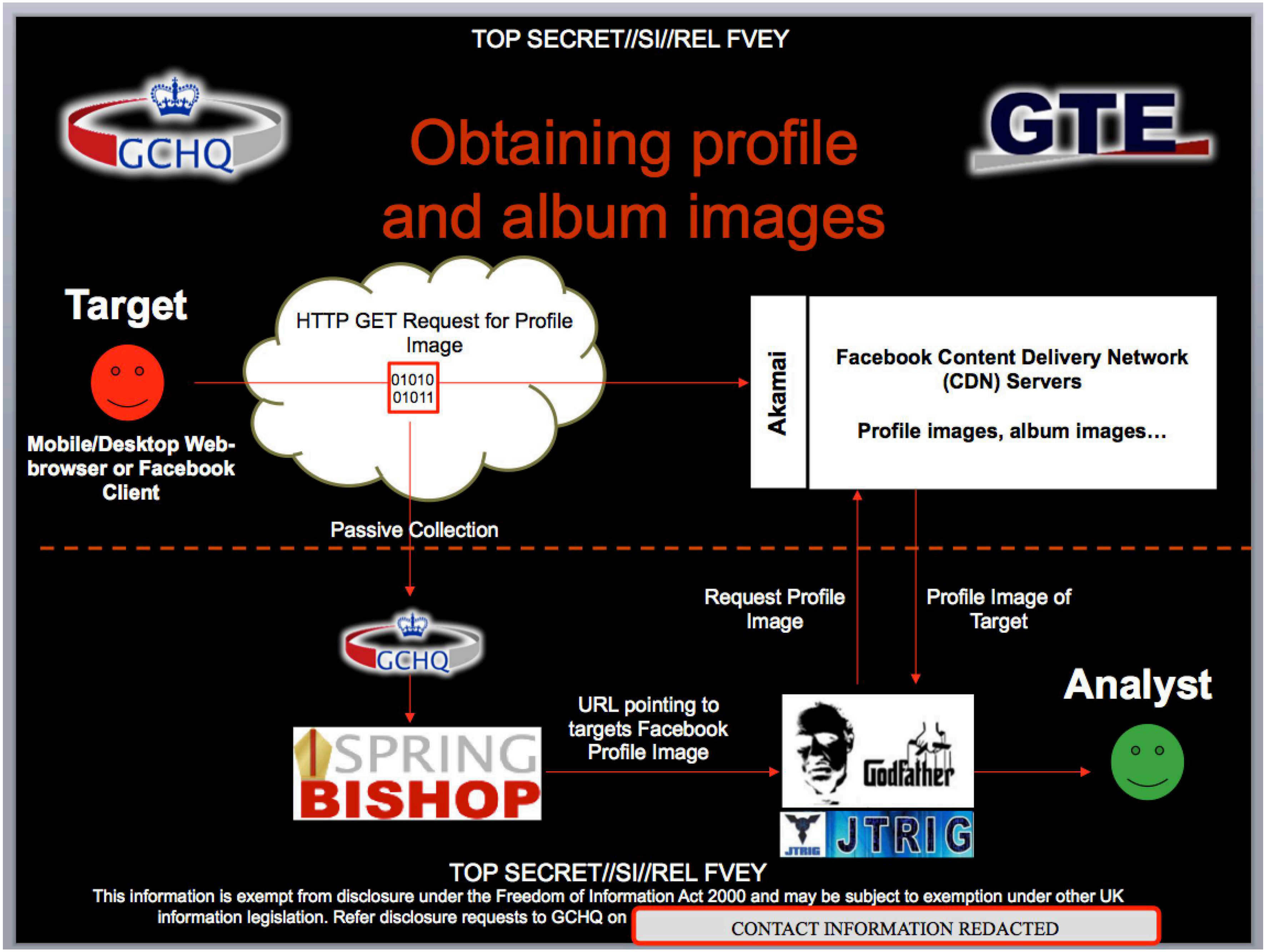
It is possible to dissect the CDN URL's generated by Facebook in order to extract the Facebook User ID of the user whose picture the file pertains to. For example, below is a typical profile image URL:

http://**profile.ak.fbcdn.net**/hprofile-ak-sf2p/hs621.snc3/27353_ REDACTED _2215_q.jpg

The text highlighted in green specifically relates to the specific server within Facebooks CDN. And the text highlighted in yellow is the users Facebook User ID.

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//SI//REL FVEY

GCHQ

GTE

Obtaining profile and album images

Target

Mobile/Desktop Web-browser or Facebook Client

HTTP GET Request for Profile Image

01010
01011

Akamai

Facebook Content Delivery Network (CDN) Servers

Profile images, album images…

Passive Collection

GCHQ

SPRING BISHOP

URL pointing to targets Facebook Profile Image

Request Profile Image

Profile Image of Target

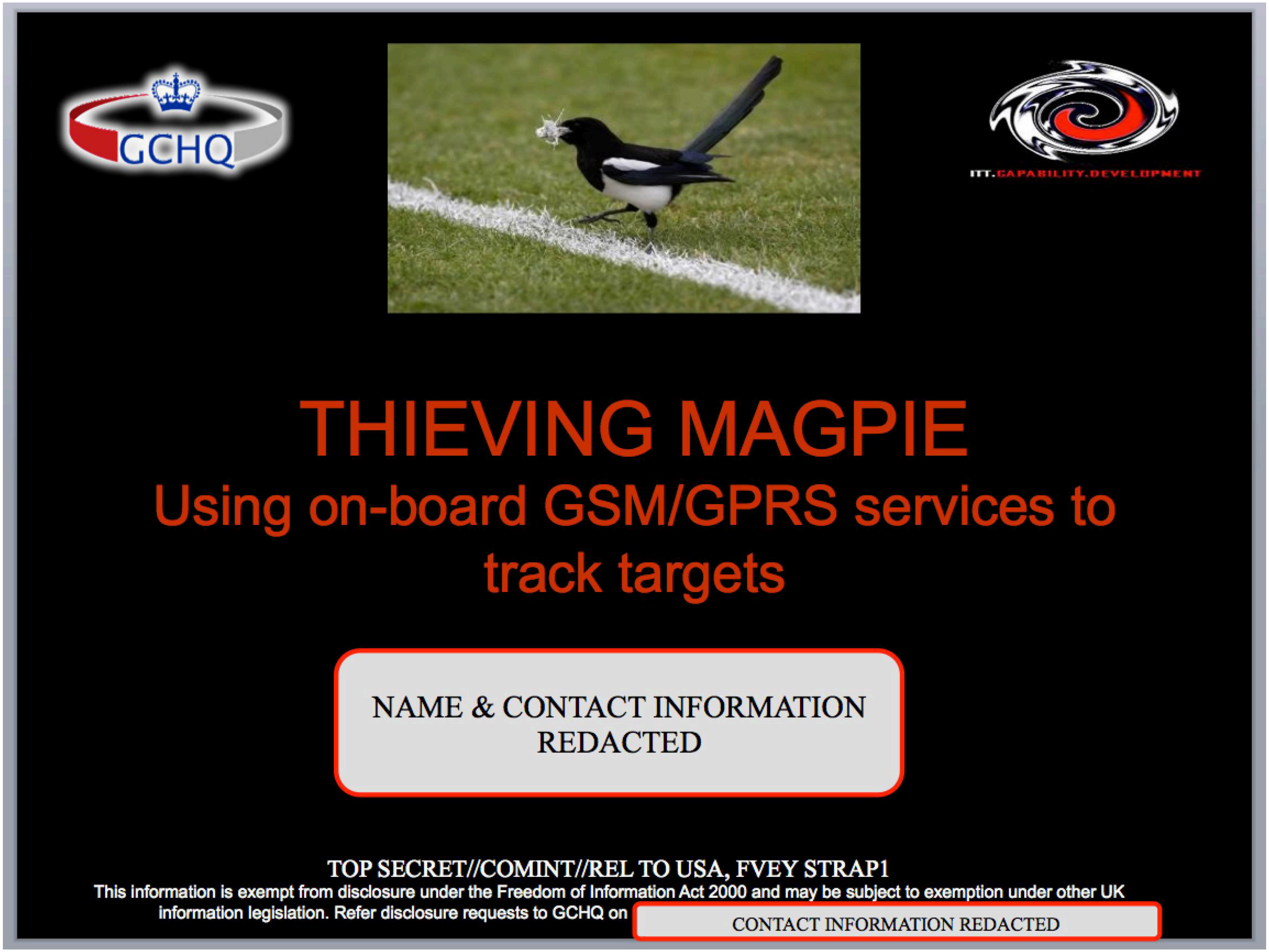
Godfather

JTRIG

Analyst

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



GCHQ
ITT.CAPABILITY.DEVELOPMENT

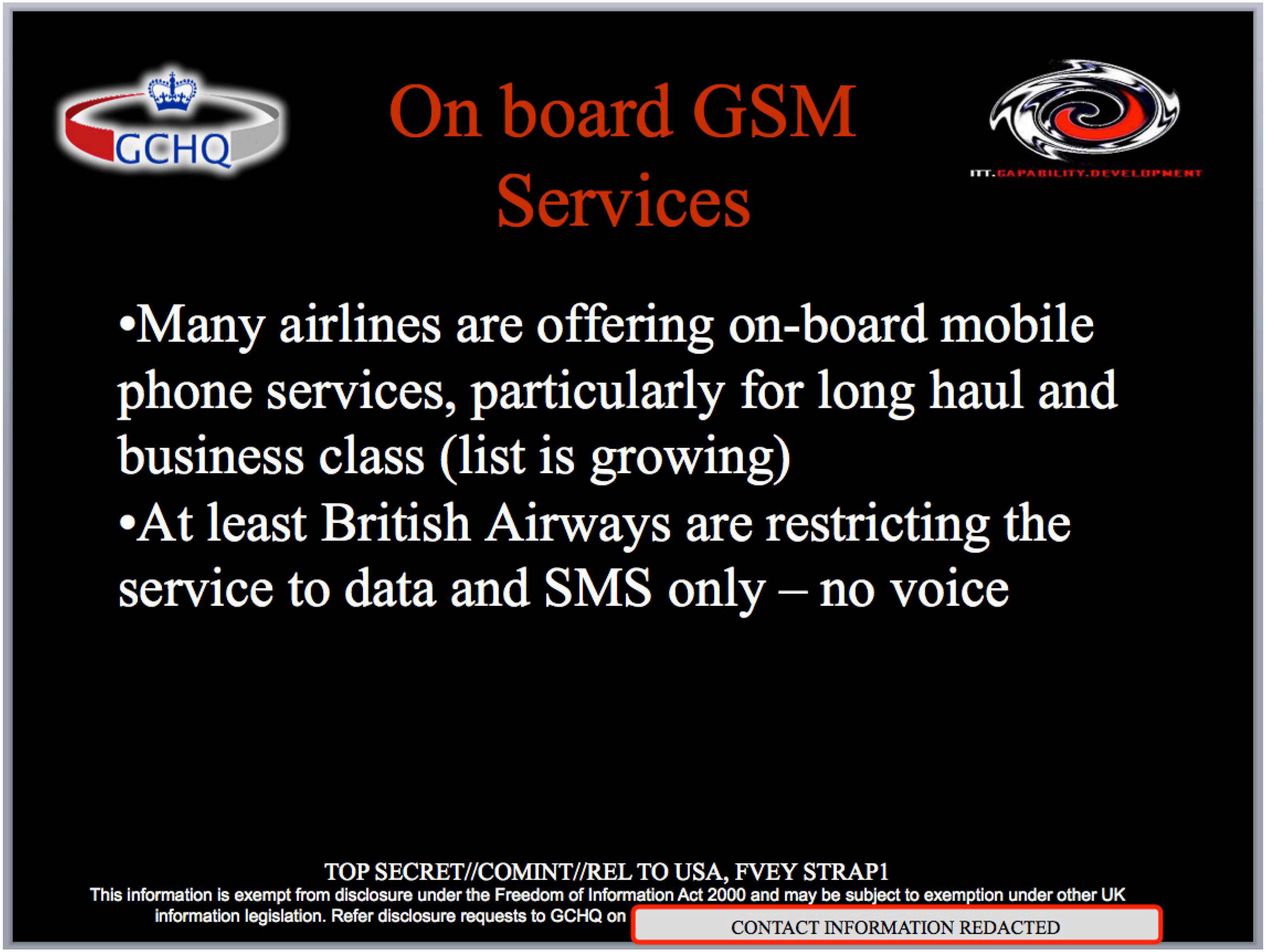
THIEVING MAGPIE

Using on-board GSM/GPRS services to track targets

NAME & CONTACT INFORMATION REDACTED

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



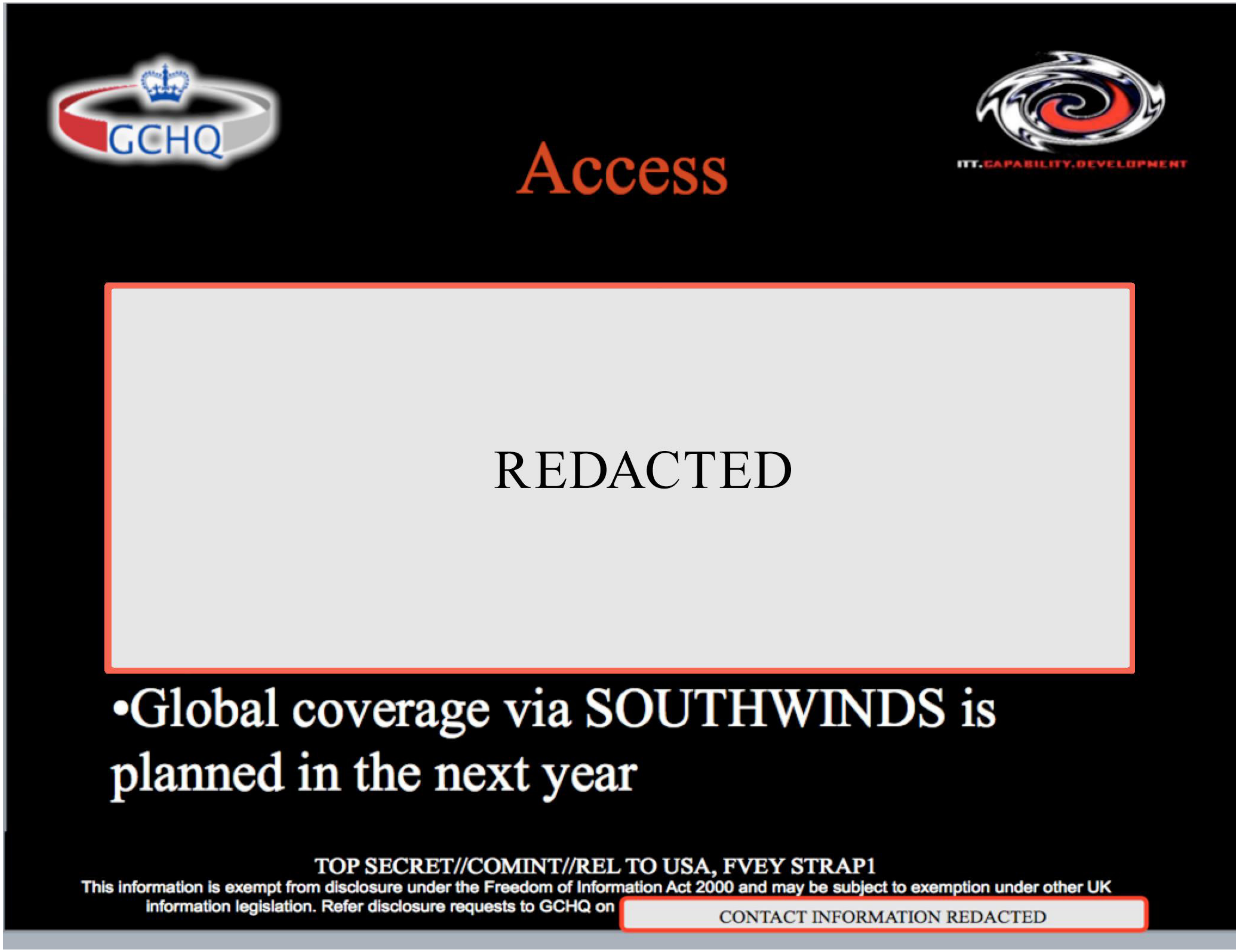
On board GSM Services

ITT.CAPABILITY.DEVELOPMENT

- Many airlines are offering on-board mobile phone services, particularly for long haul and business class (list is growing)
- At least British Airways are restricting the service to data and SMS only – no voice

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



GCHQ

ITT.CAPABILITY.DEVELOPMENT

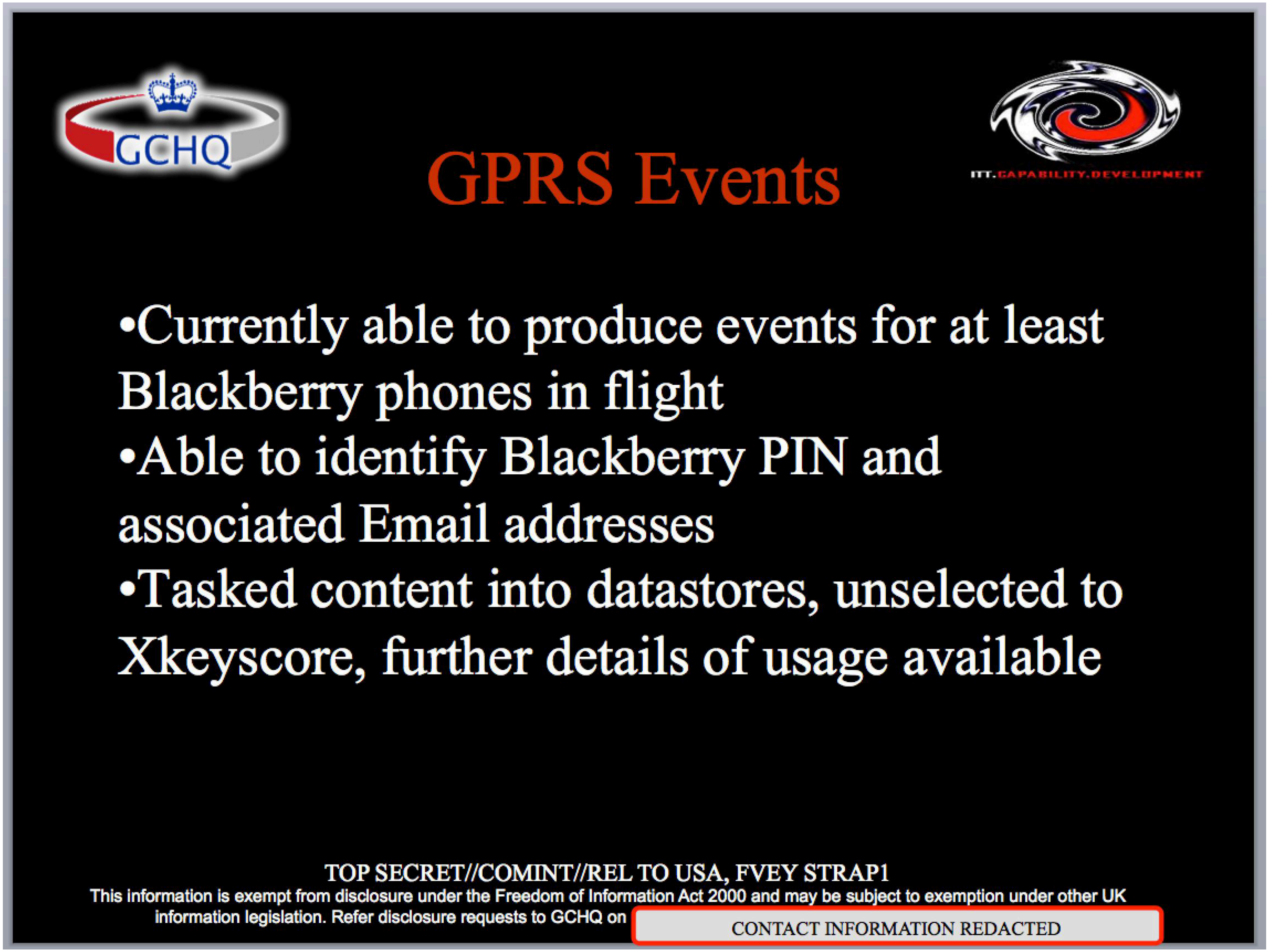
Access

REDACTED

- Global coverage via SOUTHWINDS is planned in the next year

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

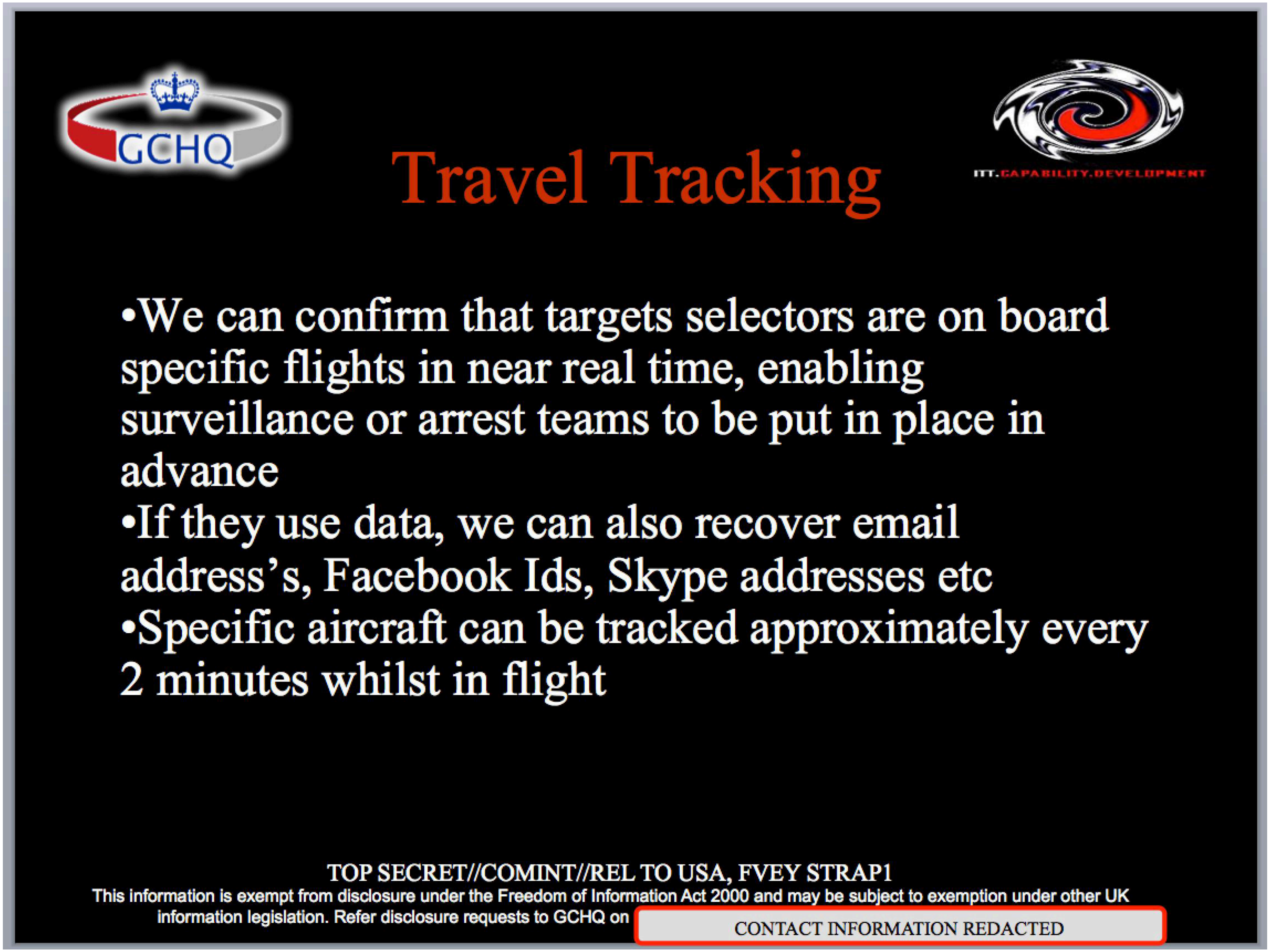

GCHQ
ITT.CAPABILITY.DEVELOPMENT

GPRS Events

- Currently able to produce events for at least Blackberry phones in flight
- Able to identify Blackberry PIN and associated Email addresses
- Tasked content into datastores, unselected to Xkeyscore, further details of usage available

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



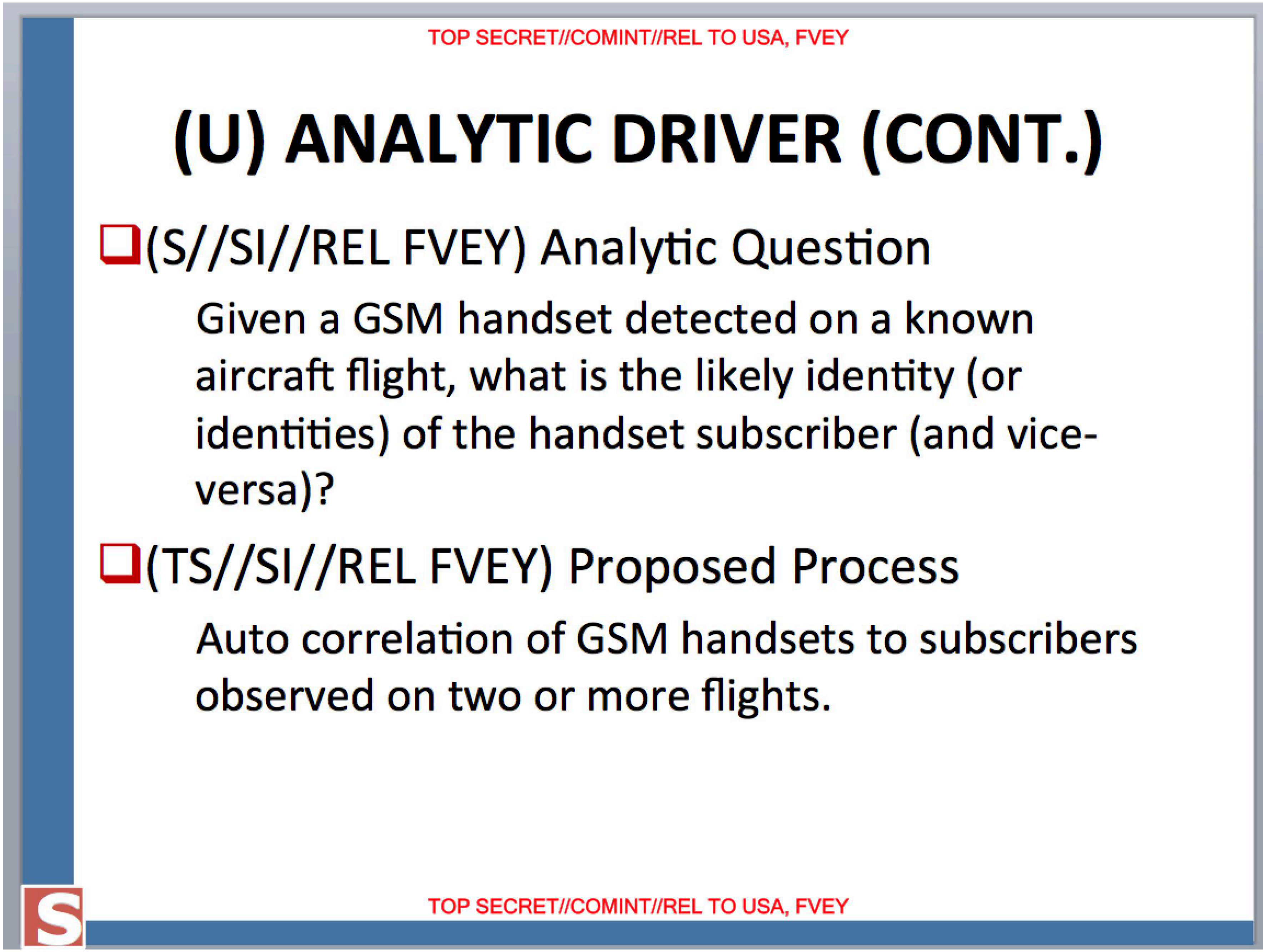
GCHQ
ITT.CAPABILITY.DEVELOPMENT

Travel Tracking

- We can confirm that targets selectors are on board specific flights in near real time, enabling surveillance or arrest teams to be put in place in advance
- If they use data, we can also recover email address's, Facebook Ids, Skype addresses etc
- Specific aircraft can be tracked approximately every 2 minutes whilst in flight

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED



TOP SECRET//COMINT//REL TO USA, FVEY

(U) ANALYTIC DRIVER (CONT.)

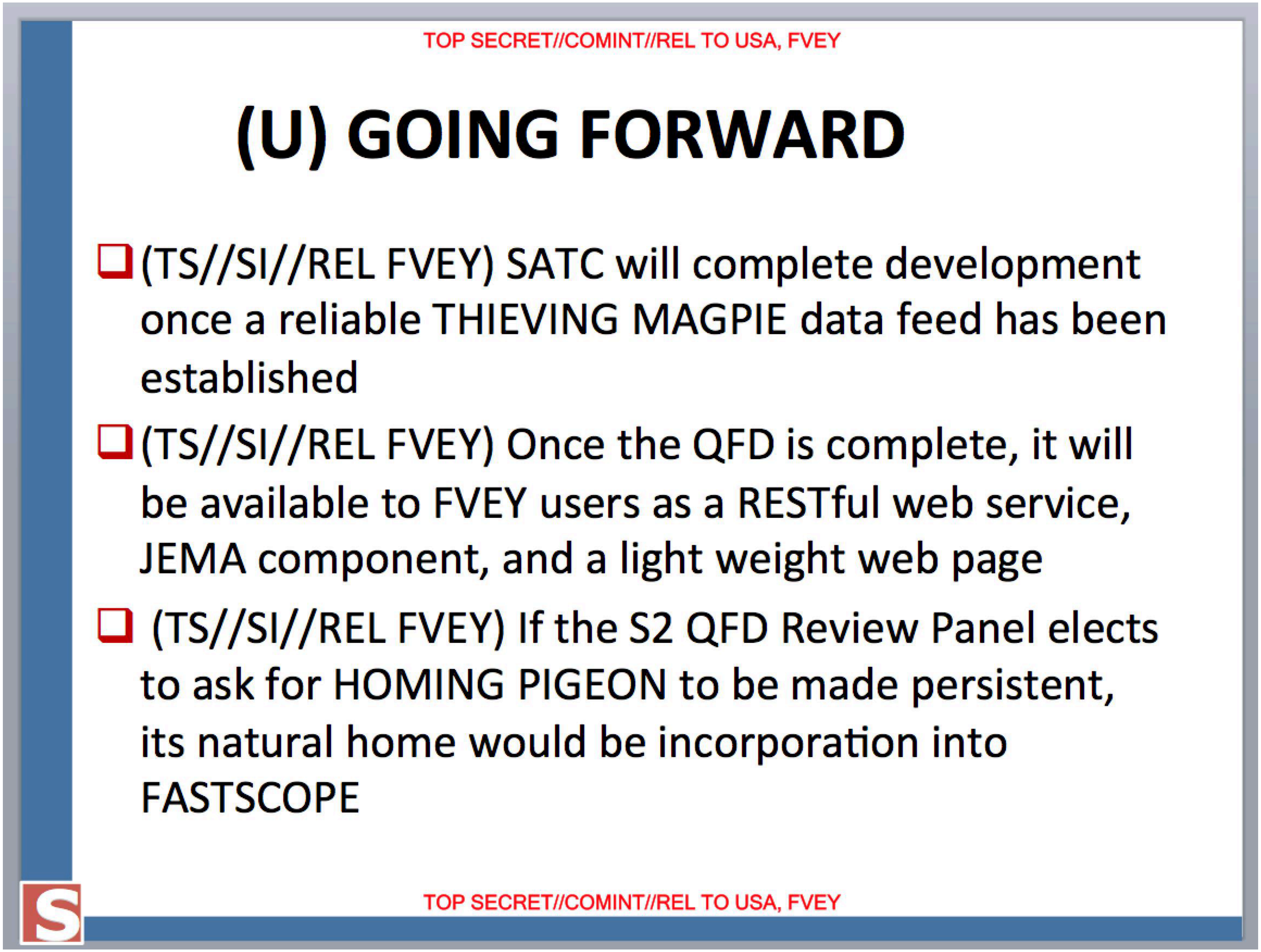
□(S//SI//REL FVEY) Analytic Question

Given a GSM handset detected on a known aircraft flight, what is the likely identity (or identities) of the handset subscriber (and vice-versa)?

□(TS//SI//REL FVEY) Proposed Process

Auto correlation of GSM handsets to subscribers observed on two or more flights.

TOP SECRET//COMINT//REL TO USA, FVEY



TOP SECRET//COMINT//REL TO USA, FVEY

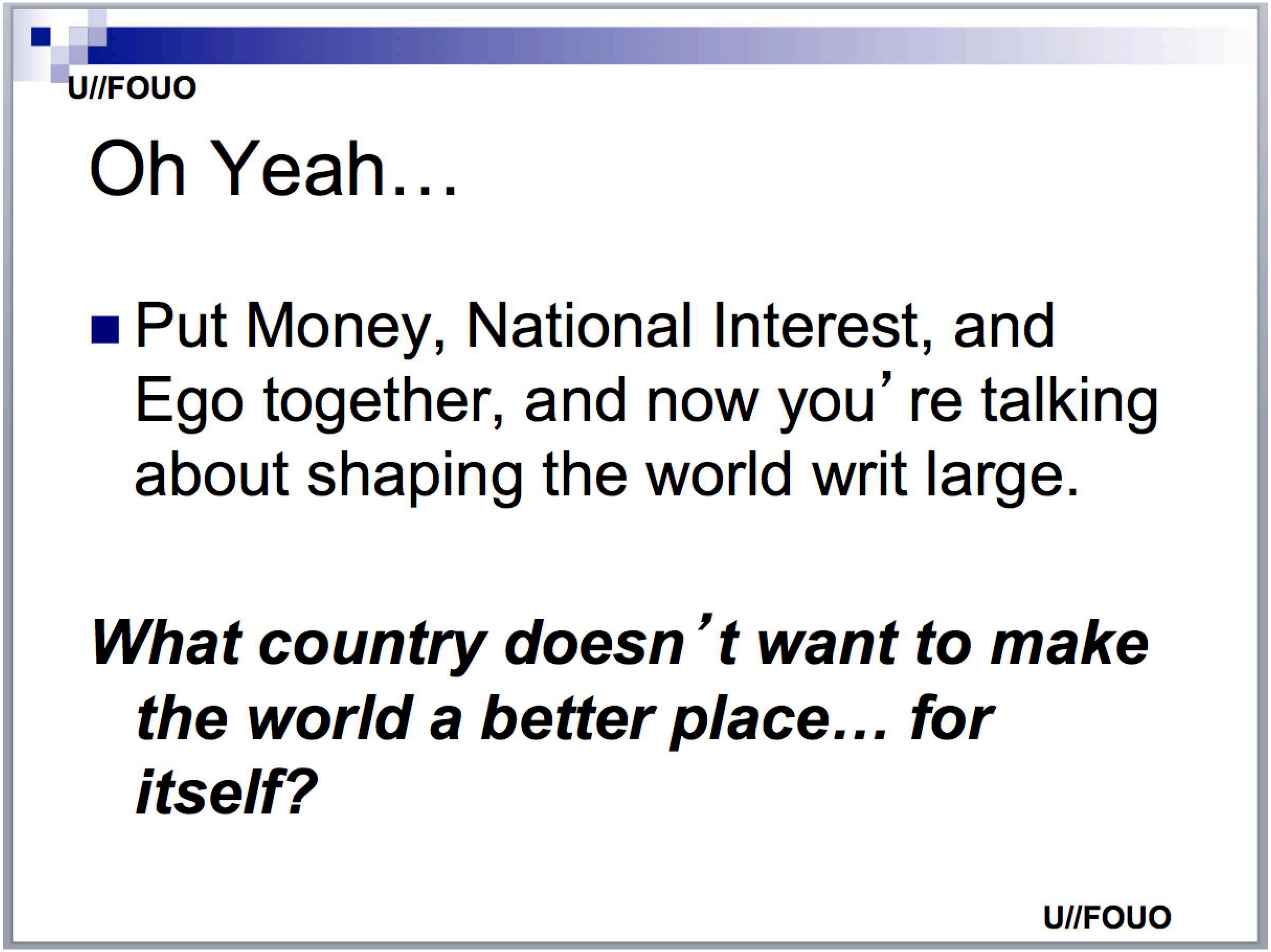
(U) GOING FORWARD

□ (TS//SI//REL FVEY) SATC will complete development once a reliable THIEVING MAGPIE data feed has been established

□ (TS//SI//REL FVEY) Once the QFD is complete, it will be available to FVEY users as a RESTful web service, JEMA component, and a light weight web page

□ (TS//SI//REL FVEY) If the S2 QFD Review Panel elects to ask for HOMING PIGEON to be made persistent, its natural home would be incorporation into FASTSCOPE

TOP SECRET//COMINT//REL TO USA, FVEY



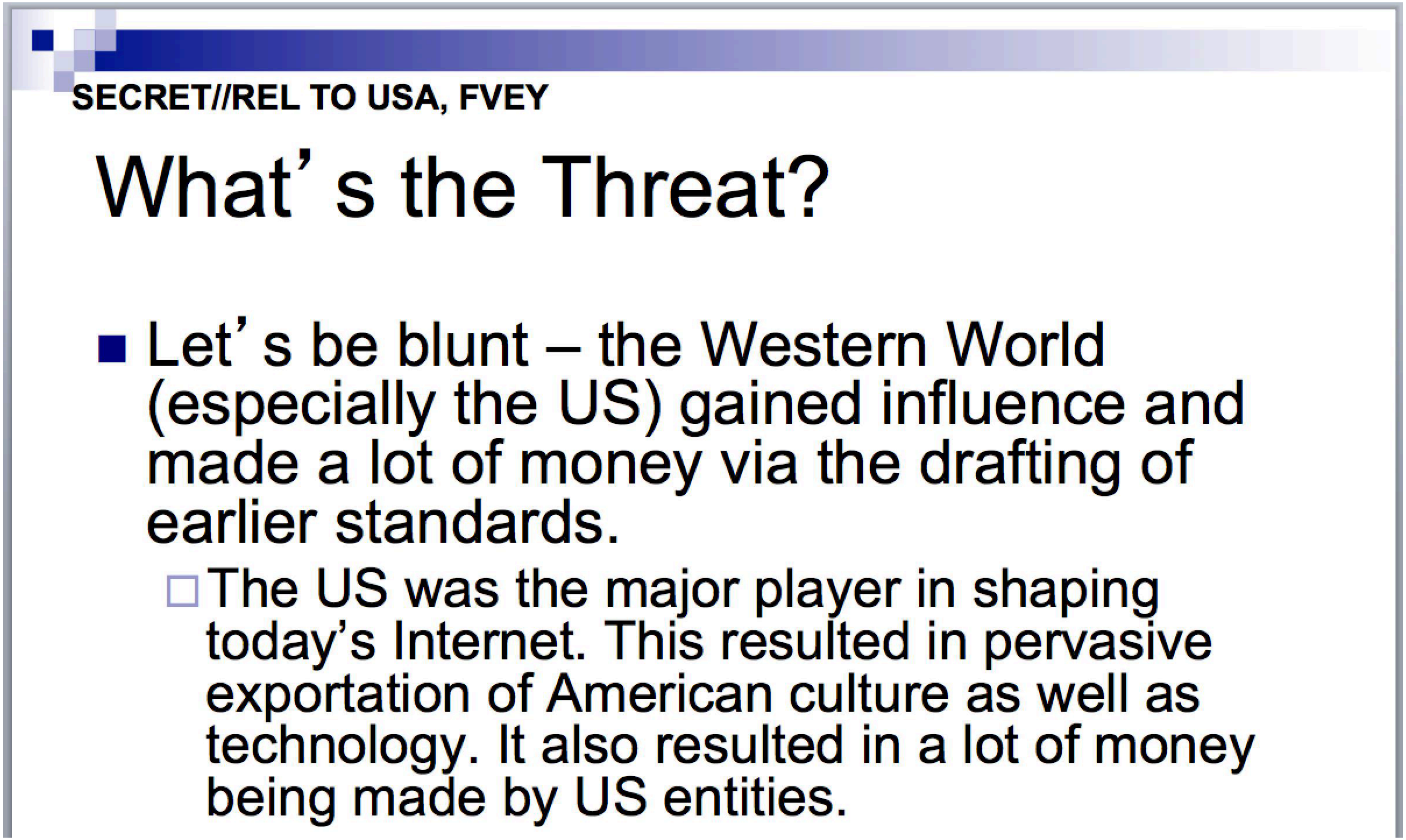
U//FOUO

Oh Yeah…

- Put Money, National Interest, and Ego together, and now you’ re talking about shaping the world writ large.

What country doesn’ t want to make the world a better place… for itself?

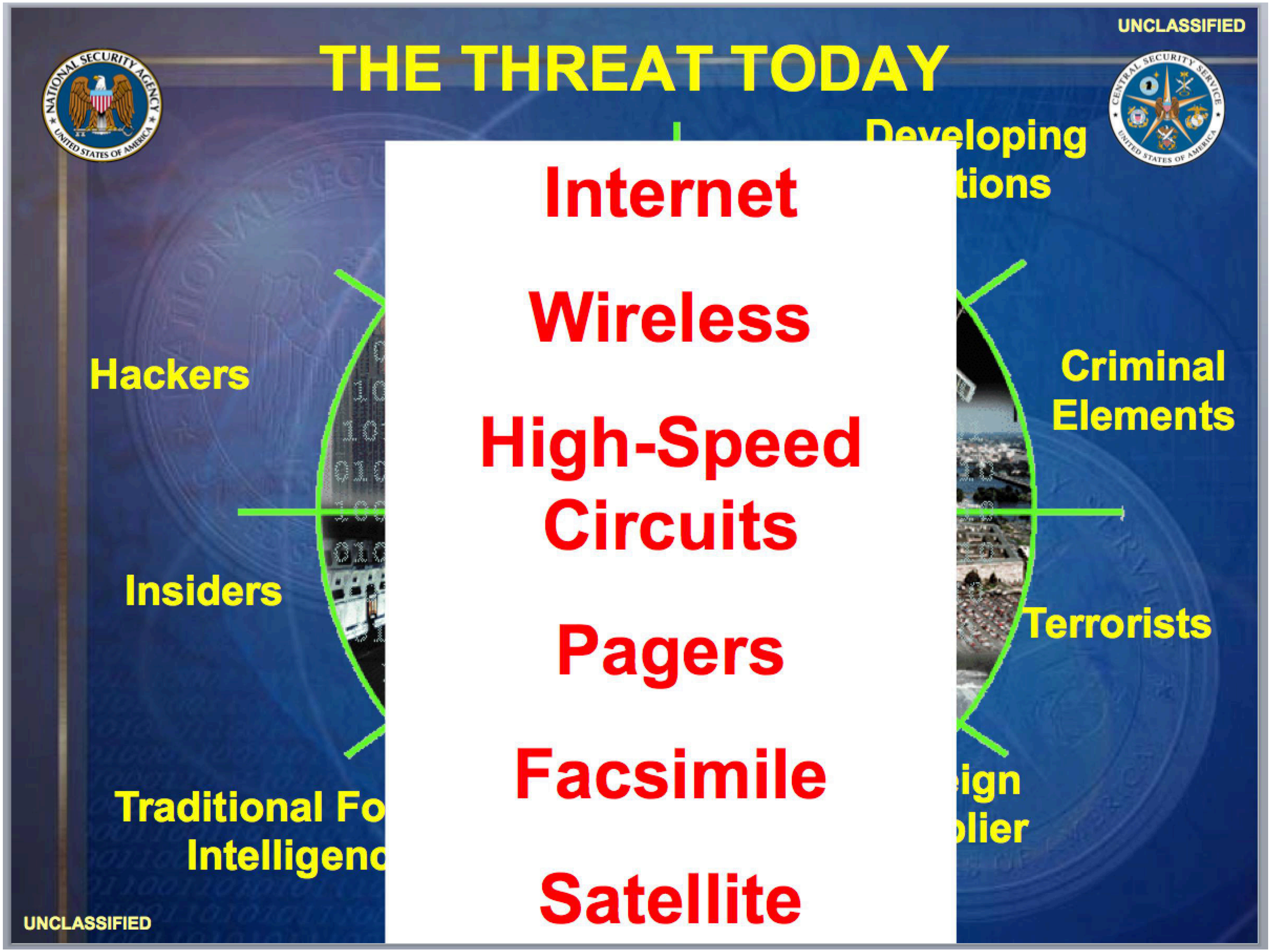
U//FOUO



SECRET//REL TO USA, FVEY

What’ s the Threat?

- Let’ s be blunt – the Western World (especially the US) gained influence and made a lot of money via the drafting of earlier standards.
  - □ The US was the major player in shaping today’s Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by US entities.



UNCLASSIFIED

THE THREAT TODAY

Developing
tions

Hackers

Criminal
Elements

Insiders

Terrorists

Traditional Fo
Intelligenc

ign
plier

UNCLASSIFIED

Internet

Wireless

High-Speed
Circuits

Pagers

Facsimile

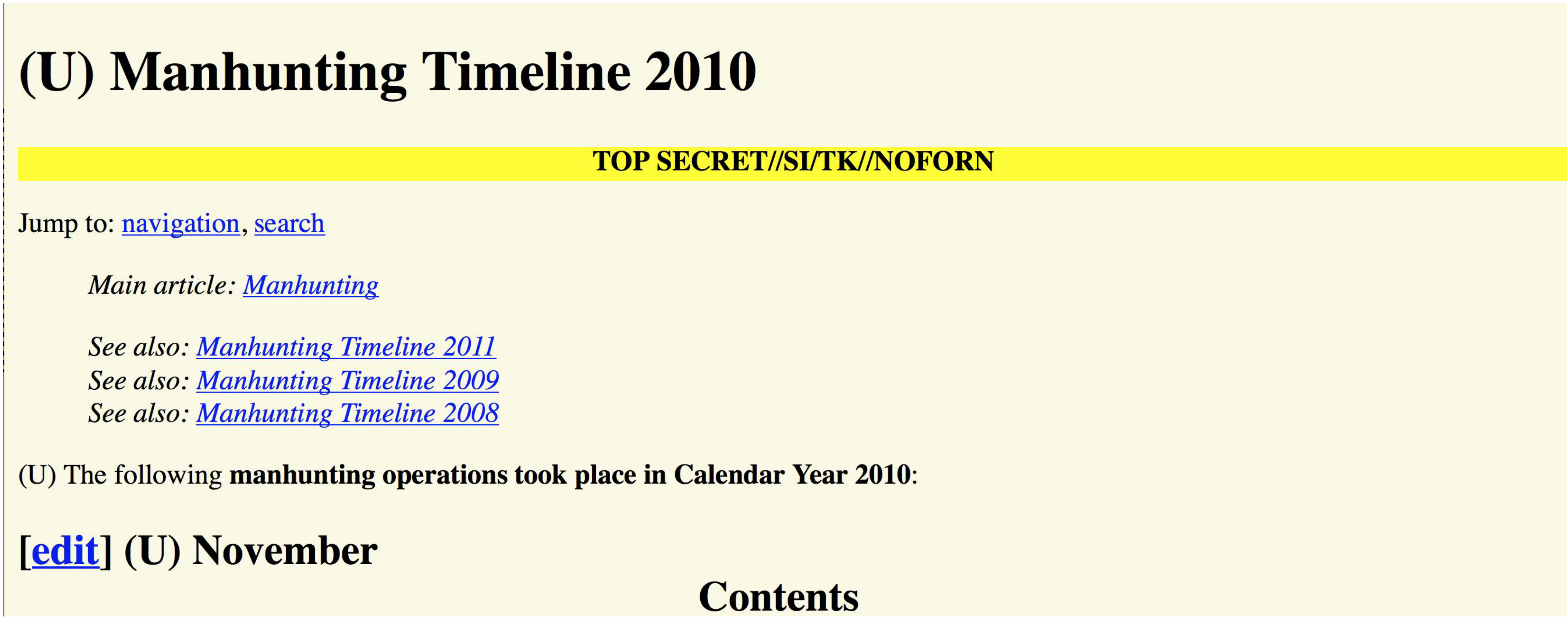
Satellite

BACKGROUND (U)

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- Viewing sexually explicit material online or using sexually explicit persuasive language when communicating with inexperienced young girls;
- Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;
- Charging an exorbitant amount of money for their speaking fees and being singularly attracted by opportunities to increase their stature; or
- Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.



(U) Manhunting Timeline 2010

TOP SECRET//SI/TK//NOFORN

Jump to: navigation, search

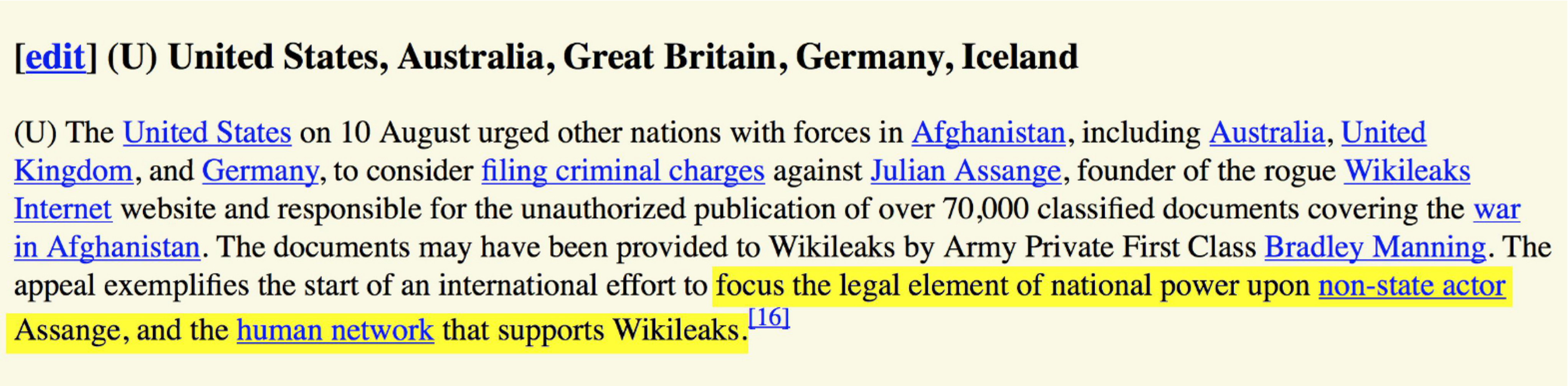
Main article: Manhunting

See also: Manhunting Timeline 2011
See also: Manhunting Timeline 2009
See also: Manhunting Timeline 2008

(U) The following **manhunting operations took place in Calendar Year 2010**:

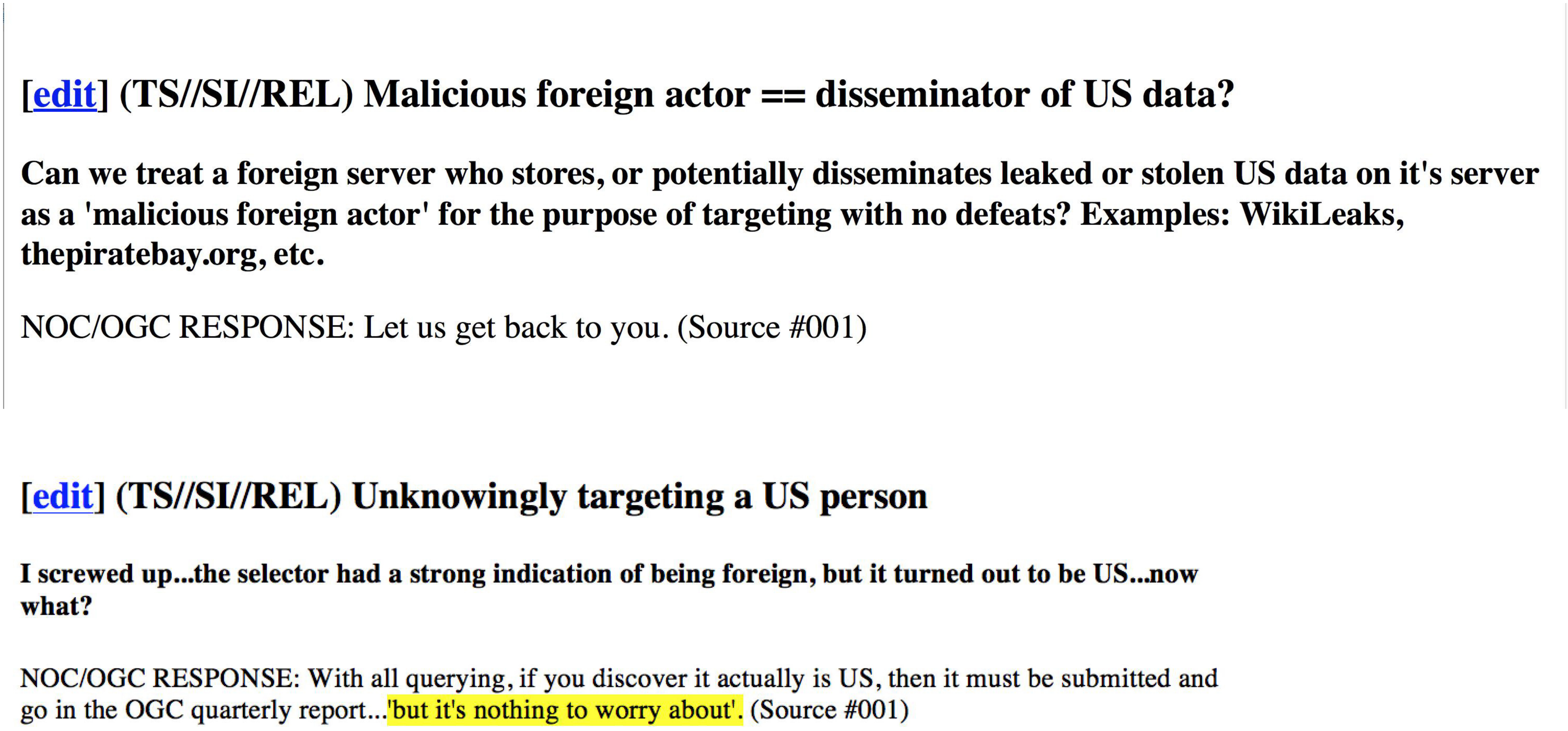
[edit] (U) November

Contents



[edit] (U) United States, Australia, Great Britain, Germany, Iceland

(U) The United States on 10 August urged other nations with forces in Afghanistan, including Australia, United Kingdom, and Germany, to consider filing criminal charges against Julian Assange, founder of the rogue Wikileaks Internet website and responsible for the unauthorized publication of over 70,000 classified documents covering the war in Afghanistan. The documents may have been provided to Wikileaks by Army Private First Class Bradley Manning. The appeal exemplifies the start of an international effort to focus the legal element of national power upon non-state actor Assange, and the human network that supports Wikileaks.[16]



[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

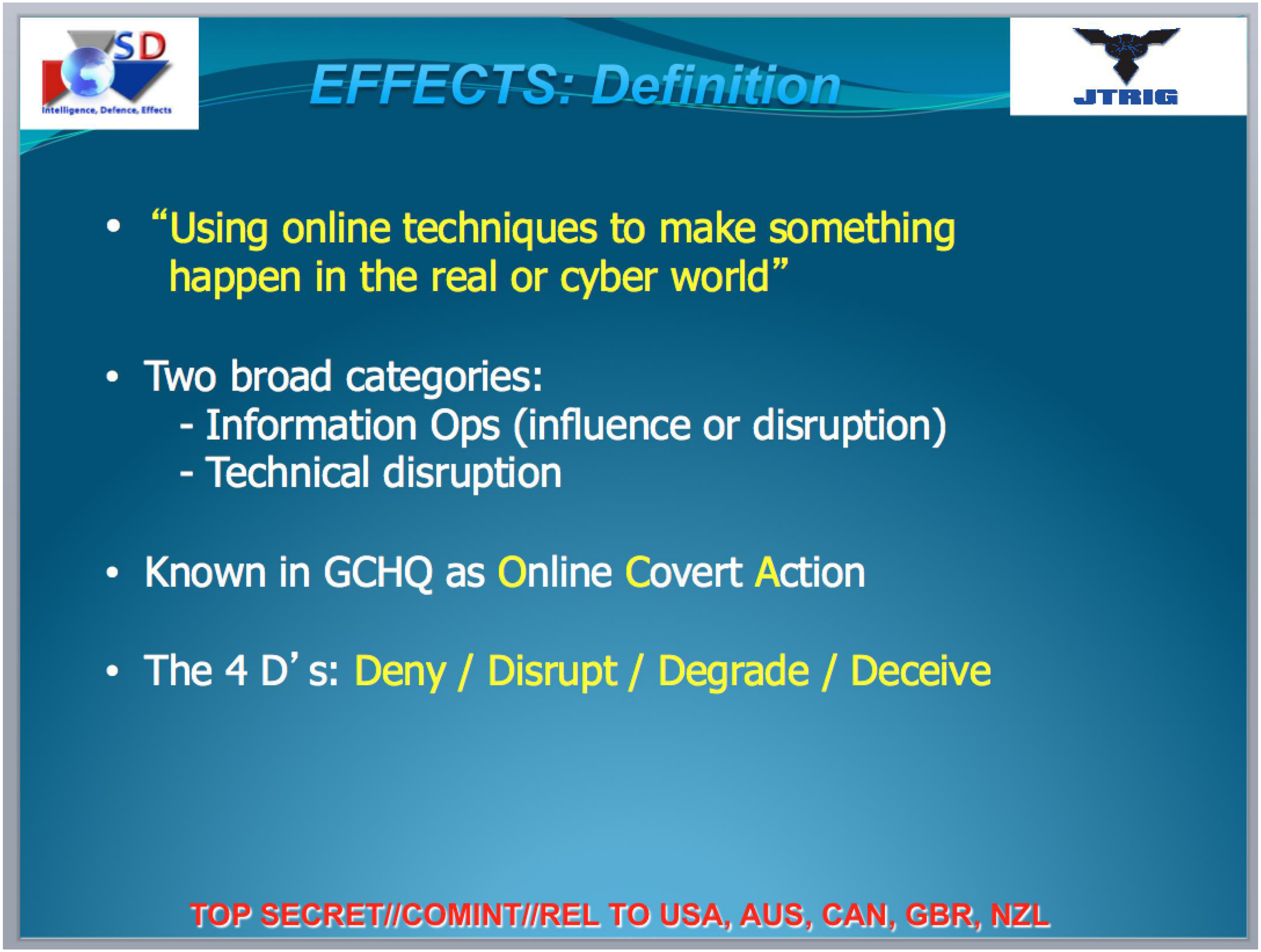
Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

[edit] (TS//SI//REL) Unknowingly targeting a US person

I screwed up...the selector had a strong indication of being foreign, but it turned out to be US...now what?

NOC/OGC RESPONSE: With all querying, if you discover it actually is US, then it must be submitted and go in the OGC quarterly report...'but it's nothing to worry about'. (Source #001)

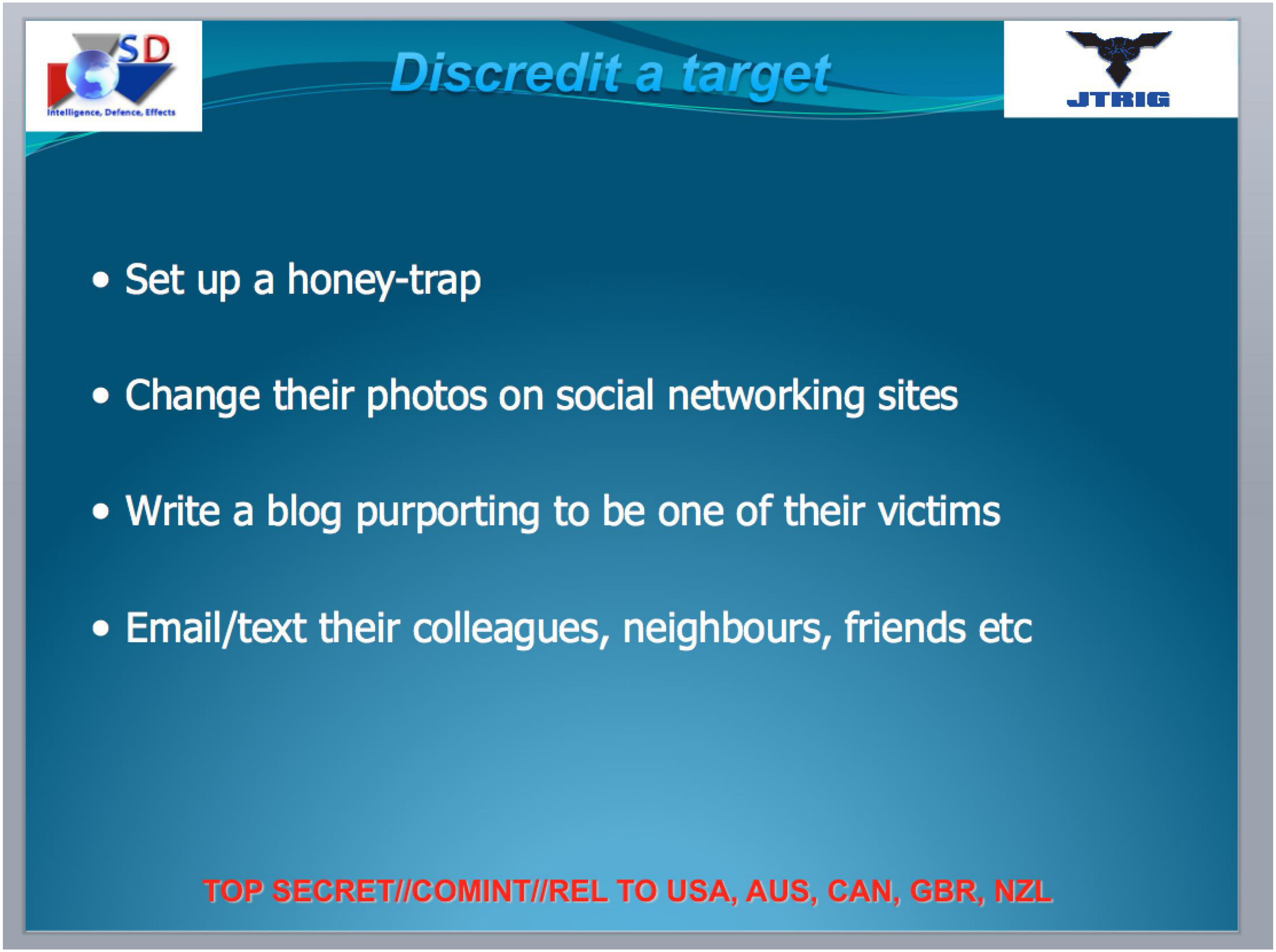


SD
Intelligence, Defence, Effects
JTRIG

EFFECTS: Definition

- "Using online techniques to make something happen in the real or cyber world"
- Two broad categories:
  - Information Ops (influence or disruption)
  - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D' s: Deny / Disrupt / Degrade / Deceive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

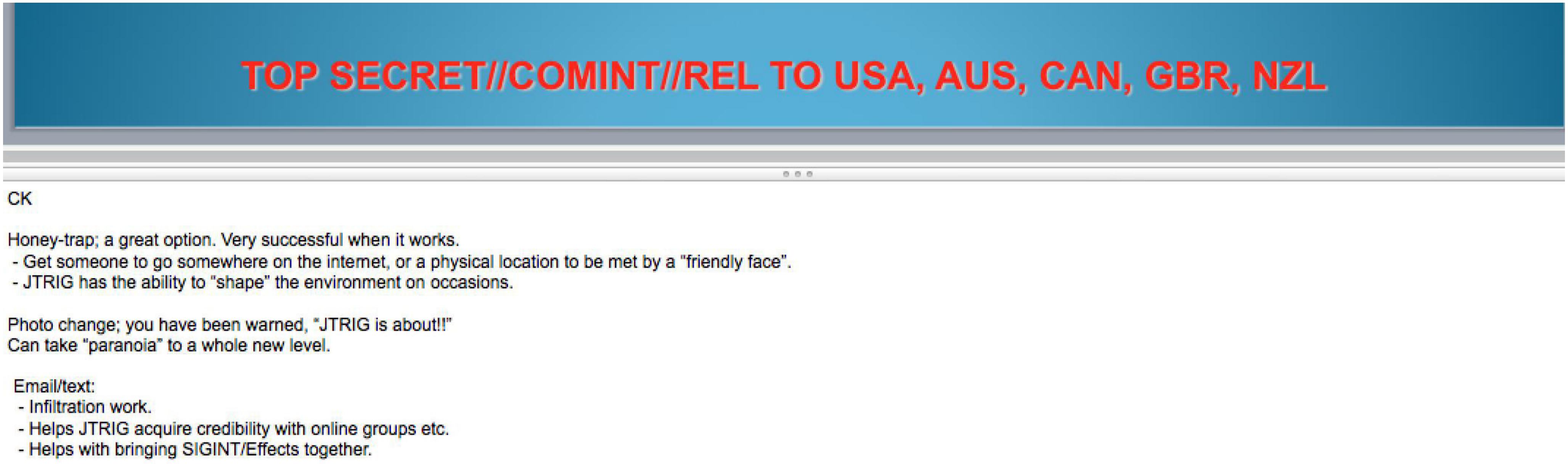


SD
Intelligence, Defence, Effects
JTRIG

Discredit a target

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



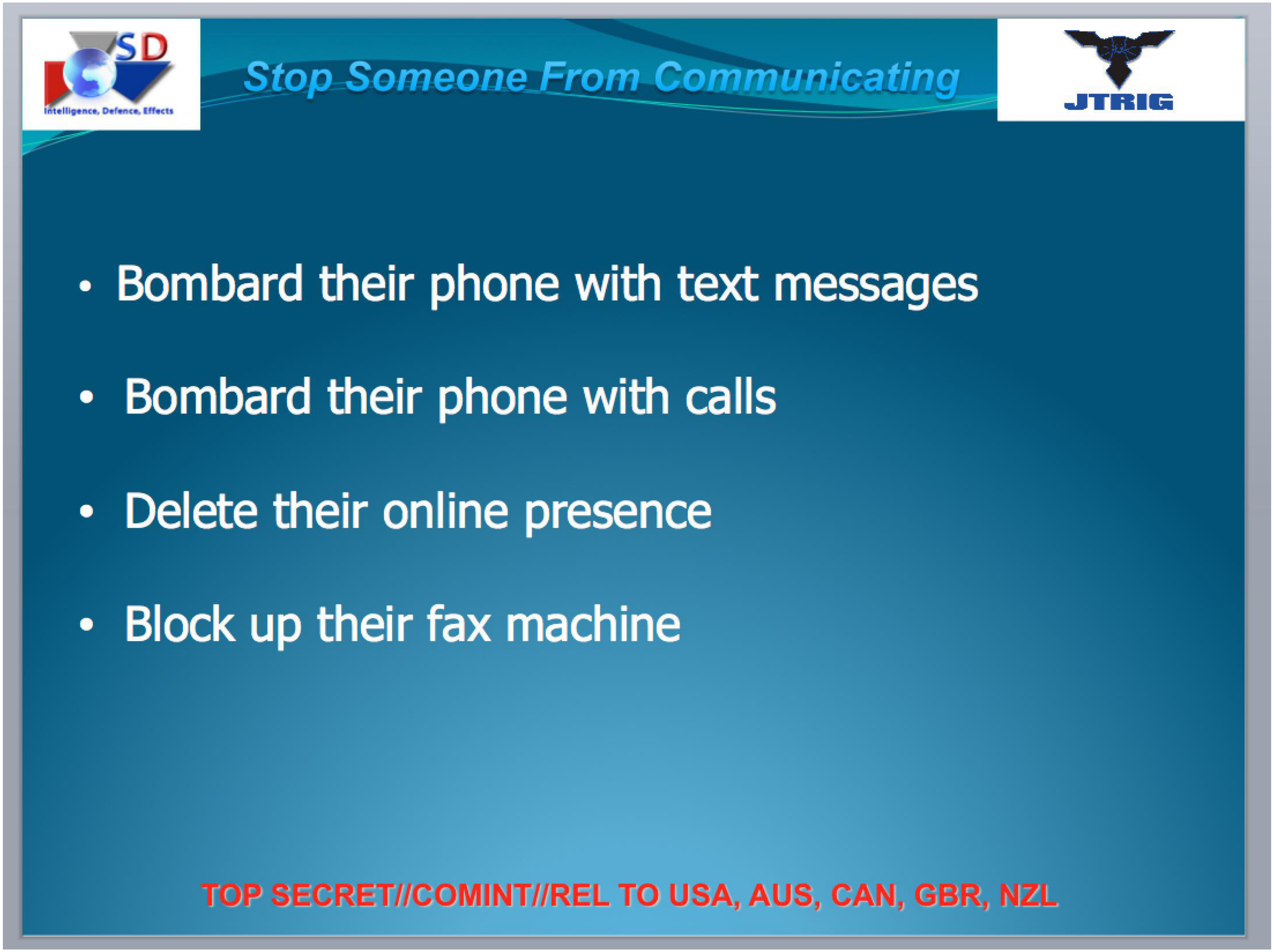
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

CK

Honey-trap; a great option. Very successful when it works.
 - Get someone to go somewhere on the internet, or a physical location to be met by a "friendly face".
 - JTRIG has the ability to "shape" the environment on occasions.

Photo change; you have been warned, "JTRIG is about!!"
Can take "paranoia" to a whole new level.

Email/text:
 - Infiltration work.
 - Helps JTRIG acquire credibility with online groups etc.
 - Helps with bringing SIGINT/Effects together.

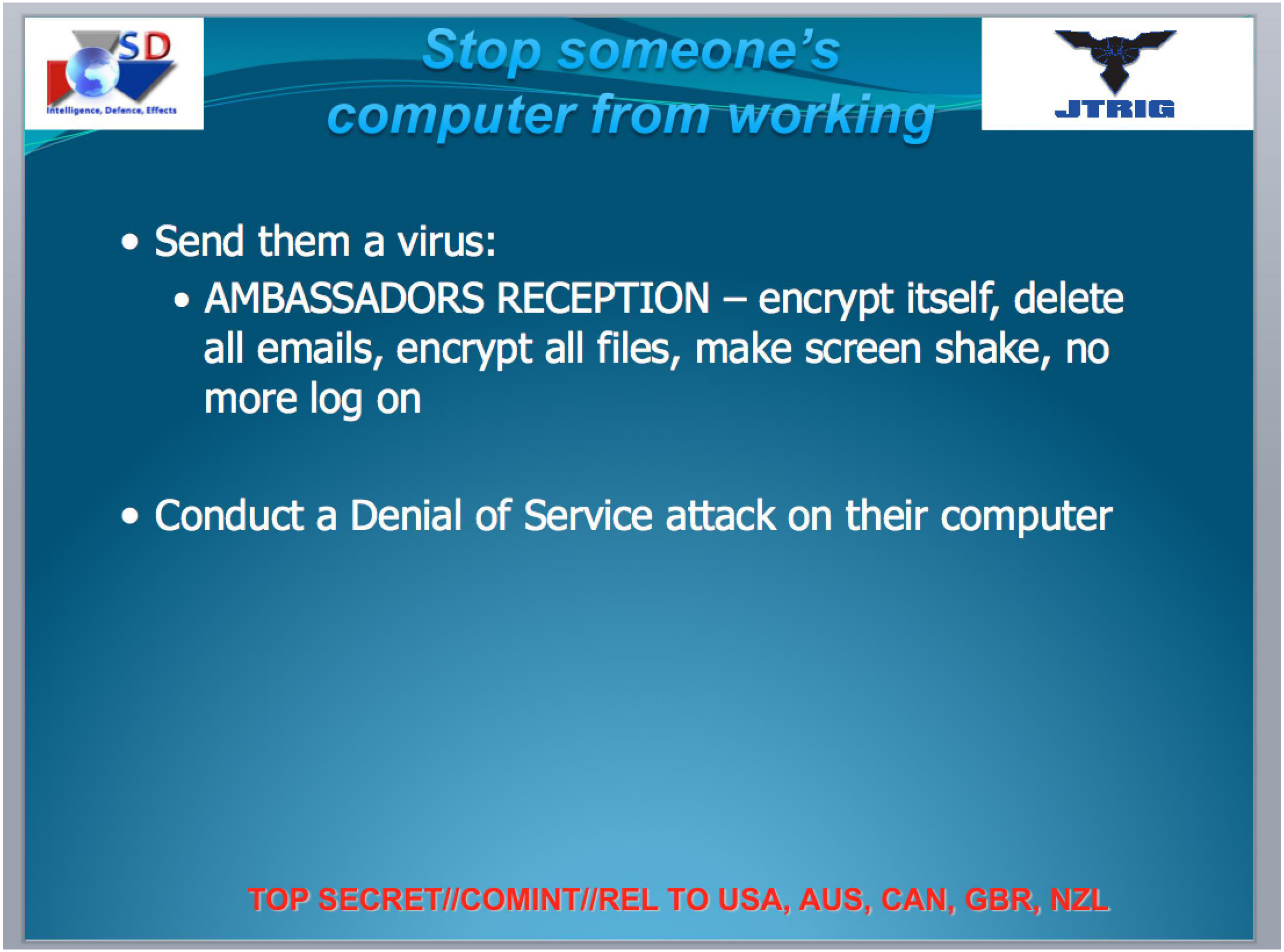


SD
Intelligence, Defence, Effects
JTRIG

Stop Someone From Communicating

- Bombard their phone with text messages
- Bombard their phone with calls
- Delete their online presence
- Block up their fax machine

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



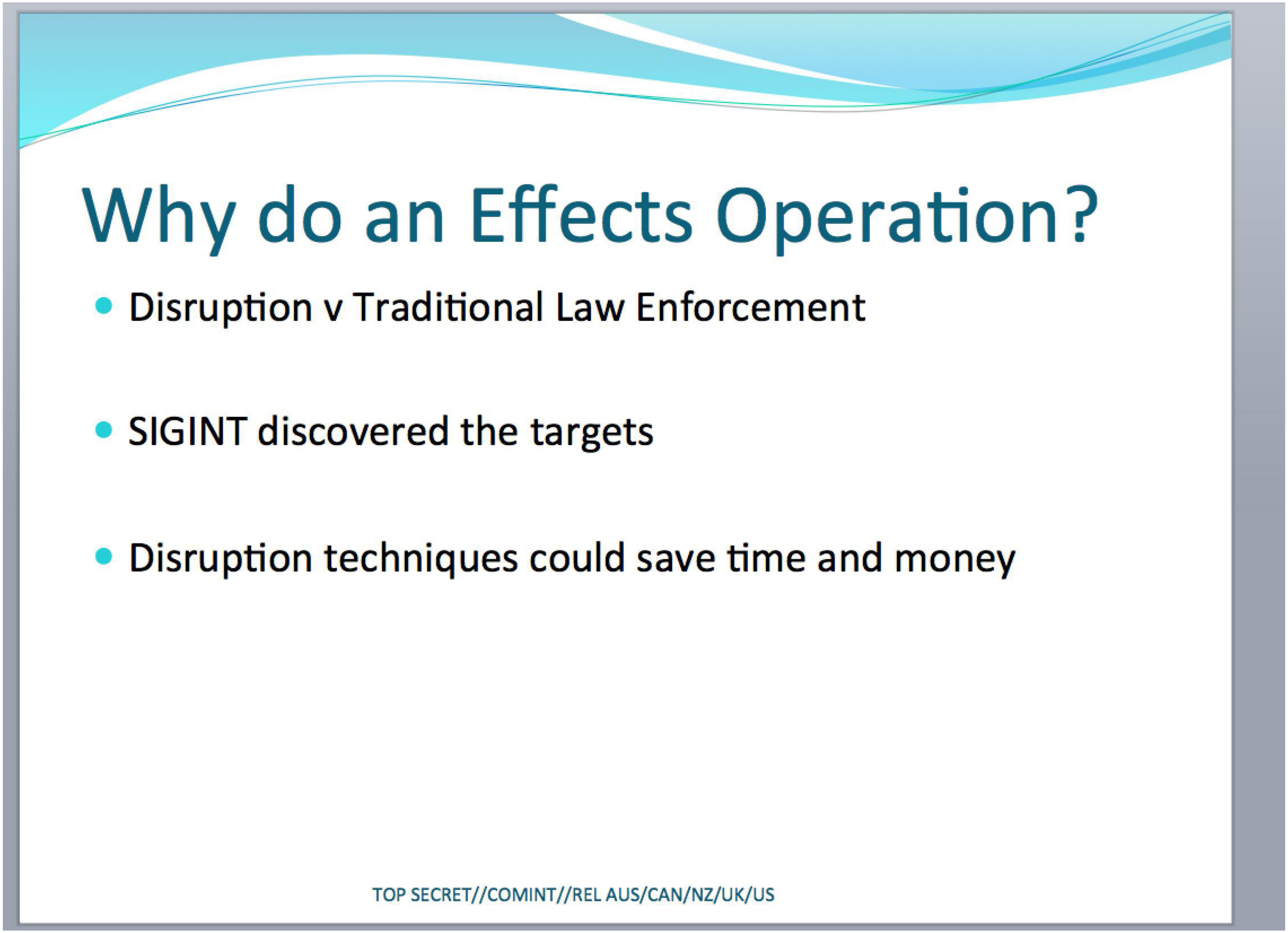
SD Intelligence, Defence, Effects

Stop someone's computer from working

JTRIG

- Send them a virus:
  - AMBASSADORS RECEPTION – encrypt itself, delete all emails, encrypt all files, make screen shake, no more log on
- Conduct a Denial of Service attack on their computer

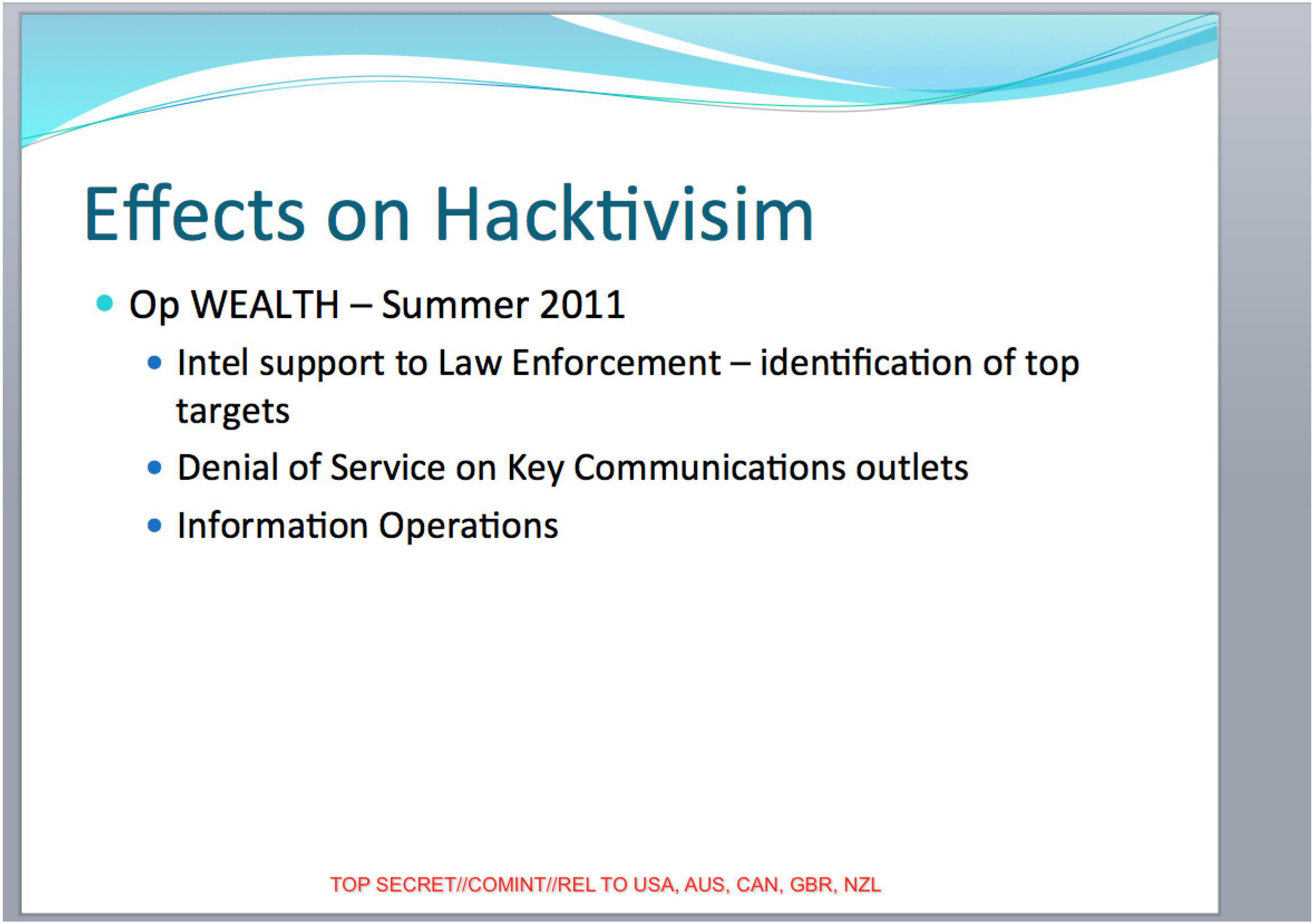
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



Why do an Effects Operation?

- Disruption v Traditional Law Enforcement
- SIGINT discovered the targets
- Disruption techniques could save time and money

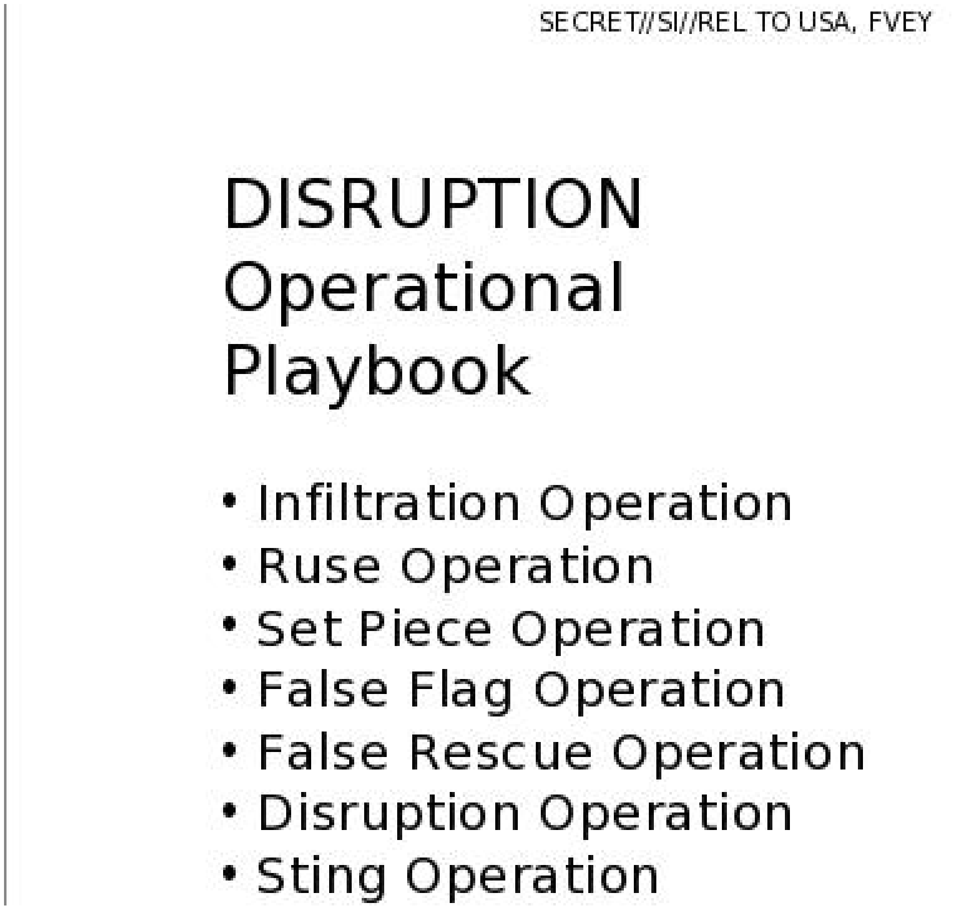
TOP SECRET//COMINT//REL AUS/CAN/NZ/UK/US



Effects on Hacktivisim

- Op WEALTH – Summer 2011
  - Intel support to Law Enforcement – identification of top targets
  - Denial of Service on Key Communications outlets
  - Information Operations

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



SECRET//SI//REL TO USA, FVEY

DISRUPTION Operational Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation